Función Pública	**Procedimiento** **Seguridad y privacidad de la información**	**Versión:**	V1
		Fecha Actualización:	6/05/2026
		Proceso asociado:	Gestión Tecnologías de la Información

1. Objetivo	Garantizar la confidencialidad, integridad y disponibilidad de la información de Función Pública, a través de la implementación de medidas técnicas, administrativas y operativas de conformidad con la normatividad vigente, con el fin de proteger los datos institucionales y mitigar los riesgos de ciberseguridad		
2. Alcance	Inicia con la verificación de la normatividad o el monitoreo de detección de novedades, continúa con la aplicación de medidas de protección para atender las novedades identificadas y finaliza con la verificación de los resultados de las actividades planificadas		
3. Lider	Jefe Oficina de Tecnologías de la Información y las Comunicaciones.	**4. Responsable**	Jefe Oficina de Tecnologías de la Información y las Comunicaciones. Oficial de Seguridad de la Información Especialistas en Seguridad Administradores de sistemas Comité de crisis Equipo de riesgo Equipo operativo

5. Deficiones

Legalidad	Cumplimiento de todas las disposiciones legales vigentes	**Integridad**	Que los datos estén completos, sean confiables y no hayan sido modificados ni alterados accidentalmente por un usuario no autorizado.
Seguridad	Protección contra riesgos y amenazas	**Disponibilidad**	Garantizar que la información, los sistemas y los recursos sean accesibles y operativos para los usuarios autorizados cuando los necesiten.
Confidencialidad	Reserva de información no pública	**Datos personales**	Cualquier tipo de información que identifica o hace identificable a una persona física, directa o indirectamente. Esto incluye datos básicos como nombres, direcciones o números de teléfono
SIEM	Security Information and Event Management. Es una solución de ciberseguridad que centraliza, analiza y correlaciona en tiempo real los registros (logs) y eventos de seguridad de toda la infraestructura de TI de una empresa.	**EDR**	Endpoint Detection and Response. es una solución de ciberseguridad avanzada que supervisa continuamente los dispositivos finales (ordenadores, servidores, móviles) para detectar, analizar y bloquear amenazas en tiempo real.
Vulnerabilidad	Infracción de seguridad que implica la copia, transferencia o movimiento intencionados y no autorizados de datos desde un equipo, dispositivo, aplicación, servicio o base de datos.	**Cumplimiento Normativo**	Proceso mediante el cual una organización cumple con leyes, regulaciones y estándares establecidos para proteger sus datos, sistemas y comunicaciones contra accesos no autorizados.

6. Políticas de Operación

1- Con el fin de garantizar la confidencialidad de toda la información institucional, especialmente aquella clasificada como sensible o confidencial, se debera proteger contra accesos no autorizados, así mismo el personal solo podrá acceder a la información estrictamente necesaria para el cumplimiento de sus funciones.

2- Para garantizar que la información no sea alterada, manipulada o destruida de forma no autorizada, se implementarán controles que aseguren la exactitud, coherencia y confiabilidad de la información.

3- Se implementarán planes de continuidad, respaldos y medidas de recuperación ante incidentes, con el fin de proteger la disponibilidad de la información y los servicios asociados, asegurando que estén accesibles para los usuarios autorizados cuando se requiera.

4- La entidad dará cumplimiento a los lineamientos establecidos en la normatividad vigente (Ley 1581 de 2012, estándares internacionales (ISO/IEC 27001 e ISO/IEC 27701) y los lineamientos del MSPI – MinTIC, en materia de seguridad y privacidad de la información.

5- Con el fin de detectar, prevenir y responder oportunamente ante incidentes de seguridad y posibles vulneraciones a la privacidad de los datos, se realizarán monitoreos de forma permanente y sistemática los activos de información, la infraestructura tecnológica y los sistemas de información.

7. Riesgos

Cod.	Nombre	
No 51	Posibilidad de afectación reputacional por queja, demanda o sanción de los grupos de valor y/o entes de control debido a pérdida de confidencialidad en activos que contiene información con carácter personal administrados por la OTIC	https://www.funcionpublica.gov.co/documents/61037/651966/2025-03-12_Anexo_mapa_fichas_riesgos_tecnologias_infomracion_051_v2.pdf/6e7330a8-3505-2250-7d27-80b623faa87a?version=1.1&t=1752067923639&previewFileIndex=1
No 53	Posibilidad de afectación reputacional por quejas de grupos de valor y/o sanciones de entes de control debido a pérdida de Integridad (modificación no autorizada) de la información o configuración de los servicios gestionados por la OTIC causados por posible ataque informático, falla eléctrica, errores de configuración, error humano en la aplicación de procedimientos, falla tecnológica, vulnerabilidades conocidos o desconocidos en el software y hardware	https://www.funcionpublica.gov.co/documents/61037/651966/2025-03-12_Anexo_mapa_fichas_riesgos_tecnologias_infomracion_051_v2.pdf/6e7330a8-3505-2250-7d27-80b623faa87a?version=1.1&t=1752067923639&previewFileIndex=1
No 57	Posibilidad de pérdida reputacional por quejas y sanciones de entes de control debido a pérdida de disponibilidad o incumplimiento de los ANS (acuerdos de niveles de servicio) de los servicios y sistemas de información administrados por la OTIC, causados por incidentes de seguridad fuera de control	https://www.funcionpublica.gov.co/documents/61037/651966/2025-03-12_Anexo_mapa_fichas_riesgos_tecnologias_infomracion_057_v2.pdf/2544dbb5-d986-40be-0038-e85ea2852a19?version=1.1&t=1752067873810&previewFileIndex=1
No 110	Posibilidad de afectación reputacional por divulgación no autorizada debido a pérdida de confidencialidad de la información reservada o clasificada almacenada en las bases de datos del aplicativo por la integridad pública.	https://www.funcionpublica.gov.co/documents/61037/651966/2025-03-12_Anexo_mapa_fichas_riesgos_tecnologias_infomracion_057_v2.pdf/2544dbb5-d986-40be-0038-e85ea2852a19?version=1.1&t=1752067873810&previewFileIndex=1

8. Indicadores

No.	Nombre	
Ficha 24	Implementación de controles del modelo de seguridad y privacidad de la información	https://www.funcionpublica.gov.co/web/intranet/mop/informacion-estrategica-y-estadistica/indicadores
Ficha 34	Sensibilización y capacitación en seguridad digital	https://www.funcionpublica.gov.co/web/intranet/mop/informacion-estrategica-y-estadistica/indicadores
No aplica	No aplica	No aplica
No aplica	No aplica	No aplica

9. Descripción del procedimiento

Convenciones:

Inicio	Actividad	Actividad de control	Decisión	Actividad paralela	Sistema de Información	Otro proceso	Fin

No.	Iconografía	Actividad	Descripción de la actividad	Tiempo	Responsable	Control	Registro/formato	Sistema de Información
1	Inicio	Implementar medidas de seguridad y privacidad de la información	Implementa medidas de seguridad y privacidad de la información tales como monitoreo y detección y verificación de cumplimiento normativo	Permanentemente, Inmediato al identificar la necesidad	Jefe Oficina de las Tecnologías de la Información Oficial de Seguridad de la Información Administradores de sistemas	Validación de que cumple criterios para activar el procedimiento Asignación de número de caso Monitoreo permanente	Registros de monitoreo, detección y verificación normativa	Proactivanet Correo electrónico corporativo
2	Cumplimiento normativo / Monitoreo	¿Es monitoreo y detención permanente o cumplimiento normativo?	Verificar	Permanente de manera inmediata.	Jefe Oficina de las Tecnologías de la Información Oficial de Seguridad de la Información Administradores de sistemas	No aplica	No aplica	No aplica
3		Realizar monitoreo	Monitorea permanente y vigila sistemáticamente los activos de información, infraestructura y sistemas para detectar, prevenir y responder a incidentes Garantiza el acceso a la información y servicios mediante continuidad operativa, respaldos y recuperación ante incidentes.	Actividad continua y permanente	Oficial de Seguridad de la Información Administrador de sistemas o red. Soporte técnico	Monitoreo automatizado mediante herramientas SIEM. Supervisión del cumplimiento de protocolos de respuesta ante incidentes. Validación mensual de integridad de los registros de auditoría.	Registro de eventos e incidentes de seguridad. Bitácora de monitoreo diario. Informe de alertas generadas y acciones tomadas. Reporte de incidentes Registro de validación de logs o evidencias digitales.	Plataforma SIEM Sistemas de detección y prevención de intrusos Consolas de antivirus EDR Herramientas de gestión de vulnerabilidades.
4		Verificar la solicitud o situación identificada	Verifica la situación a partir del análisis, reportes, o actividades de monitoreo, e identifica la posible causa e impacto que genera sobre la seguridad y privacidad de la información.	Inmediato al momento de detectar el evento o anomalía.	Comité de crisis Equipo de riesgo Equipo operativo	Aplicación del procedimiento de notificación de incidentes o no conformidades.	Correo electrónico formal No de requerimiento	Sistemas de información, misionales,apoyo a la información y aplicativos. Proactivanet
5	NO / SI	¿Es por confidencialidad?	Si la situación identificada es por confidencialidad continua en el ítem 4 Si no es por confidencialidad, continúa en ítem 5	Inmediato al momento de detectar el evento o anomalía.	Comité de Crisis Equipo de Riesgo Equipo Operativo	No aplica	Correo electrónico formal No de requerimiento	No aplica
6		Realizar protección de confidencialidad	Proteger la información sensible y confidencial, garantizando que solo el personal autorizado acceda según sus funciones.	Tiempos de atención se ajustarán según la severidad del incidente.	Oficial de Seguridad de la Información Administradores de sistemas (dueño de la informacion) Responsables del servicio tecnológico	Políticas de acceso, acuerdos de confidencialidad, control de permisos	Listados de usuarios autorizados, acta de compromiso de confidencialidad	Sistemas de información, misionales, apoyo a la información y aplicativos Sistemas de información, Aplicativos
7	NO / SI	¿Es por integridad?	Si la situación identificada es por integridad continua en el ítem 6 Si no es por integridad, continúa en ítem 7	Inmediato al momento de detectar el evento o anomalía.	Comité de Crisis Equipo de Riesgo Equipo Operativo	No aplica	Correo electrónico formal No de requerimiento	No aplica
8		Realizar proteccion de integridad	Implementa controles que eviten la alteración, manipulación o destrucción no autorizada de la información	Tiempos de atención se ajustarán según la severidad del incidente.	Oficial de Seguridad de la Información Administradores de sistemas (dueño de la informacion) Responsables del servicio tecnológico	Política de copias de respaldo Procedimientos de back y recuperación de desastres. Uso de controles criptográficos para garantizar la disponibilidad de la información en los sistemas, Hash, control de cambios	Registro de backups en la herramienta. Caso proactivanet Bitácoras de cambios	Sistemas de información, misionales, apoyo a la información y aplicativos Sistemas de información, Aplicativos
9	NO / SI	¿Es por disponibilidad?	Si la situación identificada es por disponibilidad continua en el ítem 8 Si no es por disponibilidad, continúa en ítem 9	Inmediato al momento de detectar el evento o anomalía.	Comité de Crisis Equipo de Riesgo Equipo Operativo	No aplica	Correo electrónico formal No de requerimiento	No aplica
10		Realizar proteccion de disponibilidad	Monitorea permanente y vigila sistemáticamente los activos de información, infraestructura y sistemas para detectar, prevenir y responder a incidentes Garantiza el acceso a la información y servicios mediante continuidad operativa, respaldos y recuperación ante incidentes.	Pruebas de respaldo programadas (mensual y a demanda).	Oficial de Seguridad de la Información Administradores de sistemas (dueño de la informacion) Responsables del servicio tecnológico	Planes de continuidad, pruebas de restauración.	Actas de pruebas Logs de recuperación. Plan de restauracion de bakup	Sistemas de información, misionales, apoyo a la información y aplicativos Sistemas de información, Aplicativos
11		Realizar protección de datos personales	Implementa y mantiene medidas organizativas y técnicas que garanticen la confidencialidad, integridad y disponibilidad de los datos personales, conforme a la legislación vigente como la Ley de protección de datos personales(incluye recolección, tratamiento, almacenamiento, acceso, transferencia y eliminación segura de datos personales).	Tiempos de atención se ajustarán según la severidad del incidente.	Oficial de Seguridad de la Información DBA Administradores de sistemas (dueño de la informacion) Responsables del servicio tecnológico	Validación de consentimiento informado de los titulares de datos en cada sistema de Información. Cifrado de datos personales en tránsito y reposo. Control de accesos y trazabilidad.	Formatos de consentimiento de tratamiento de datos. Reporte de incidentes de seguridad de datos personales. Listado de usuarios con acceso a datos personales. Informes de auditoría de protección de datos.	Sistemas de información, misionales, apoyo a la información y aplicativos Sistemas de información, Aplicativos
12		Verificar cumplimiento normativo	Garantiza que la entidad cumpla con todas las leyes, regulaciones y normativas y su seguimiento, como leyes de protección de datos, internacionales, políticas internas y requisitos contractuales con terceros.	Permanente	Oficial de Seguridad de la Información Control Interno Responsables de cada proceso afectado por normativa	Monitoreo de cambios legislativos y regulatorios. Actualizaciones cuando cambien las normativas Auditorías internas Revisión de proveedores con acceso a información sensible o personal.	Acta o informe de cierre del proceso. Registro de incidentes cerrados. Bitácora de respaldo y eliminación segura. Formato de aprobación del responsable de seguridad.	Acta o informe de cierre del proceso. - Registro de incidentes cerrados. - Bitácora de respaldo y eliminación segura. - Formato de aprobación del responsable de seguridad. Sistemas de información, Aplicativos
13		Finalizar proceso Veriicar resultado actividades planificadas	Verifica que todas las actividades planificadas se hayan ejecutado correctamente , evaluando la posibilidad del riesgo, aplicación de controles, revisión de incidentes y actualización de registros revisando que haya sido tratada conforme a las políticas institucional del cumplimiento de las medidas de seguridad.	1 a 2 días posteriores a la conclusión de las actividades principales o al cierre del ciclo de revisión	Oficial de Seguridad de la Información	Verificación de cumplimiento de políticas y procedimientos de seguridad. Validación de que los registros y respaldos estén completos. Confirmación de cierre por parte del responsable designado.	Acta o informe de cierre del proceso. Lista de verificación de cumplimiento (checklist). Registro de incidentes cerrados.	Proactivanet
14		Salvaguardar la información	Una vez finalizadas las actividades, verifica que los soportes y registros de la trazabilidad de cada actividad reposen en la TRD oficial o en los sistemas de información respectivos	Permanentemente	Jefe Oficina de las Tecnologías de la Información Oficial de Seguridad de la Información Administradores de sistemas Comité de crisis Equipo de riesgo Equipo operativo	Verificar que todos los registros, cambios realizados y soportes se encuentren guardados en la TRD oficial en los sistemas de información respectivos.	Acta o informe de cierre del proceso. Lista de verificación de cumplimiento (checklist). Registro de incidentes cerrados Registro de backups en la herramienta. Caso proactivanet Bitácoras de cambios.	Proactivanet TRD oficial Sistemas de información, Aplicativos

10. Diagrama de flujo

11. Documentos asociados			
Interno		Externo	
Instructivo cifrado información confidencial	https://www.funcionpublica.gov.co/web/intranet/mop/gestion-de-las-tecnologias-de-la-informacion/instructivos-protocolos	Resolución 746 11 de marzo de 2022	https://www.funcionpublica.gov.co/web/intranet/mop/gestion-de-las-tecnologias-de-la-informacion/normograma
Política general de seguridad de la información	https://www.funcionpublica.gov.co/web/intranet/mop/gestion-de-las-tecnologias-de-la-informacion/instructivos-protocolos	Ley 2157 de 2021	https://www1.funcionpublica.gov.co/web/eva/buscador?p_p_id=com_liferay_iframe_web_portlet_IFramePortlet_INSTANCE_BaHJiC6Ya8z3&_com_liferay_iframe_web_portlet_IFramePortlet_INSTANCE_BaHJiC6Ya8z3_iframe_find=FindNext&_com_liferay_iframe_web_portlet_IFramePortlet_INSTANCE_BaHJiC6Ya8z3_iframe_query=habeas%20data
No aplica	No aplica	Ley 1266 de 2008	https://www1.funcionpublica.gov.co/web/eva/buscador?p_p_id=com_liferay_iframe_web_portlet_IFramePortlet_INSTANCE_BaHJiC6Ya8z3&_com_liferay_iframe_web_portlet_IFramePortlet_INSTANCE_BaHJiC6Ya8z3_iframe_find=FindNext&_com_liferay_iframe_web_portlet_IFramePortlet_INSTANCE_BaHJiC6Ya8z3_iframe_query=habeas%20data