

	CARACTERIZACION DE PROCESOS	Código: DG-E-CARACT-050
		Vigente desde: 11/Sep/2026
		Clasificación: Información Pública
	GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Versión: 1

OBJETIVO:	Gestionar la seguridad y la privacidad de la información del Instituto mediante la implementación, operación, seguimiento, evaluación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), a través de la gestión de riesgos y la aplicación de mecanismos de control que permitan proteger los activos de información, preservar su confidencialidad, integridad, disponibilidad y privacidad, fortalecer la continuidad de los servicios misionales y asegurar el cumplimiento de los requisitos aplicables.
ALCANCE:	Inicia con la identificación de necesidades y la planificación de la seguridad y privacidad de la información; continúa con la implementación, operación, seguimiento y evaluación de los controles establecidos; y finaliza con la ejecución de acciones para la mejora continua del proceso y la optimización de los controles.
RESPONSABLE	• Director General. • Profesional con rol de Oficial de Seguridad de la Información. • Directores Regionales.

PROVEEDOR	ENTRADAS	ACTIVIDADES	PRODUCTOS / SERVICIOS / SALIDAS	CLIENTES
1. Entidades públicas y entes de control. 2. Proceso de Gestión de Infraestructura Tecnológica y Servicios Informáticos. 3. Entidades de normalización, certificación y acreditación. 4. Proceso de Gestión de Planeación Institucional. 5. Proceso de Administración del SIG. 6. Proceso de Gestión de Seguridad de la Información.	1. Normativa legal y lineamientos de seguridad de la información y seguridad digital, informes de evaluación de desempeño, Modelo de Seguridad y Privacidad de la Información (MSPI) 2. Plan Estratégico de Tecnologías de la Información (PETI) entre otros. 3. Normativa, requisitos y lineamientos relacionados con el proceso. 4. Necesidades y expectativas de las partes interesadas, contexto estratégico, Plan Estratégico (PE), directrices y estrategias institucionales, Política de Gestión de Riesgos. 5. Política y lineamientos del	P • Planificar o actualizar el Proceso de Gestión de Seguridad de la Información. • Planificar o Actualizar el Plan Estratégico de Seguridad de la Información (PESI).	• Proceso actualizado. • Documentos del proceso. • Plan de acción anual (PAA). • Lineamientos actualizados del proceso y del SGSI. • Riesgos del proceso. • Indicadores del proceso. • Planificación de la evaluación de satisfacción del cliente. • Autodiagnóstico del MSPI. • Plan Estratégico de Seguridad de la Información (PESI) formulado.	• Todos los procesos

	SIG. 6 Plan Estratégico de Seguridad de la Información (PESI).				
Proceso de Gestión de Seguridad de la Información	- Autodiagnóstico del MSPI. - Plan Estratégico de Seguridad de la Información (PESI) formulado. - Lineamientos actualizados del proceso y del SGSI. - Plan de acción anual (PAA). - Riesgos del proceso. - Documentos del proceso. - Indicadores del proceso. - Planificación de la evaluación de satisfacción del cliente.	H	- Implementar el Plan Estratégico de Seguridad de la Información (PESI). - Elaborar o actualizar la Matriz de aplicabilidad de controles asociados a la NTC /ISO/IEC 27001. - Gestionar los riesgos del proceso. - Implementar el plan de acción anual (PAA). - Implementar los documentos del proceso. - Evaluar la satisfacción del cliente.	- Plan Estratégico de Seguridad de la Información (PESI) implementado. - Matriz de aplicabilidad de controles asociados a la NTC /ISO/IEC 27001 actualizada. - Riesgos del proceso gestionados. - Plan de acción anual (PAA) implementado. - Documentos del proceso implementados. - Resultados de la evaluación de satisfacción del cliente.	1 y 2. Todos los procesos, Alta Dirección 3 y 4. Proceso de Gestión de la Planeación. 5 y 6. Proceso de Gestión de Seguridad de la Información.
1. Proceso de Gestión de Seguridad de la Información. 2. Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC.	- Plan Estratégico de Seguridad de la Información (PESI). - Matriz de aplicabilidad de controles asociados a la NTC /ISO/IEC 27001 actualizada. - Resultados de la gestión del Mapa de Riesgos. - Resultados del seguimiento a los planes de acción anual (PAA). - Resultados de la evaluación de satisfacción del cliente. - Informes de seguimiento. - Indicadores del proceso. - Modelo de Seguridad y Privacidad de la Información (MSPI).	V	Verificar: - La implementación del Plan Estratégico de Seguridad de la Información (PESI). - El estado de aplicabilidad de los controles asociados a la NTC /ISO/IEC 27001. - La gestión de riesgos de seguridad de la información. - El avance de los Planes de acción Anual (PAA). - Los resultados de la evaluación de satisfacción del cliente. - Los resultados de los informes de seguimiento. - Los resultados de los indicadores del proceso. - El estado del Modelo de Seguridad y Privacidad de la Información (MSPI). Evaluar el desempeño del proceso y del SGSI.	- Informe de Implementación del PESI. - Informe de aplicabilidad de controles asociados a la NTC/ISO /IEC 27001. - Informe del Estado del MSPI. - Información de entrada para la Revisión del Sistema Integrado de Gestión por la Alta Dirección. - No conformidades, oportunidades de mejora, cambios que afecten el SIG y necesidades de recursos. - Informes de seguimiento. - Resultado de la medición de los indicadores del proceso.	1, 2 y 3 Alta Dirección. 4 y 5 Proceso de Administración del Sistema Integrado de Gestión. 3, 6 y 7 Proceso de Gestión de Seguridad de la información.
1. Proceso de Gestión de Seguridad de la información. 2. Administración del SIG. 3. Proceso de Gestión del Sistema de Evaluación y Control 4. Entidades de	- Informe de Implementación del PESI. - Informe de aplicabilidad de controles asociados a la NTC/ISO /IEC 27001. - Informe del Estado del MSPI. - No	A	Implementar acciones correctivas, preventivas o de mejora acorde con los resultados.	- Planes de mejoramiento. - Acciones implementadas.	- Administración del SIG. - Proceso de Gestión de Seguridad de la información.

normalización, certificación y acreditación. 5. Entidades públicas y entes de control. 6. Proceso de Gestión del Relacionamento con la Ciudadanía.	conformidades, oportunidades de mejora, cambios que afecten el SIG, necesidades de recursos. 1. Informes de seguimiento. 2. Informe de auditoría del SIG. 2. Salidas de la Revisión del SIG por la Alta Dirección. 3. Informe de auditoría de Control Interno. 4. Informes de auditorías internas y externas y evaluaciones de la conformidad. 5. Informe de auditorías externas de entes de control o visitas. 6. PQRSD				
1. Proceso Gestión de Seguridad de la Información. 2. Entidades públicas y entes de control. 3. Entidades de normalización, certificación y acreditación.	1. Matriz de aplicabilidad de controles asociados a la NTC /ISO/IEC 27001 actualizada. 2. Normativa legal vigente, lineamientos de seguridad de la información e informes de evaluación de desempeño, Modelo de Seguridad y Privacidad de la Información (MSPI) entre otros. 3. Normativa y lineamientos relacionados con el proceso.	P	- Diseñar y formular los controles asociados Matriz de aplicabilidad de controles asociados a la NTC /ISO/IEC 27001. - Identificar o actualizar lineamientos asociados a la política de seguridad y privacidad de la información.	- Controles formulados de acuerdo con la Matriz de aplicabilidad de controles asociados a la NTC /ISO/IEC 27001. - Lineamientos de seguridad de la información.	- Alta Dirección. - Todos los procesos.
Proceso Gestión de Seguridad de la Información.	- Lineamientos de seguridad de la información actualizados. - Plan Estratégico de Seguridad de la Información (PESI). - Controles formulados de acuerdo con la Matriz de aplicabilidad de controles asociados a la NTC /ISO/IEC 27001.	H	- Desarrollar el Plan Estratégico de Seguridad de la Información (PESI). - Implementar los controles asociados a la Matriz de Aplicabilidad.	- Informe de ejecución del Plan estratégico de seguridad de la Información (PESI). - Informe de seguimiento de la matriz de aplicabilidad de controles.	Alta Dirección.
Proceso Gestión de Seguridad de la Información.	Informe de seguimiento de la matriz de aplicabilidad de controles.	V	Realizar monitoreo a la implementación de controles de acuerdo con lo establecido en la	Informe de monitoreo a la implementación de controles de acuerdo con lo establecido en la	Alta Dirección.

	Informe de ejecución del Plan Estratégico de Seguridad de la Información (PESI).		Matriz de Aplicabilidad de Controles. Verificar el estado del Modelo de Seguridad y Privacidad de la Información MSPI.	Matriz de Aplicabilidad de Controles. Informe del estado del Modelo de Seguridad y Privacidad de la Información MSPI.	
Proceso Gestión de Seguridad de la Información.	- Informe de monitoreo a la implementación de controles de acuerdo con lo establecido en la Matriz de Aplicabilidad de Controles. - Informe del estado del Modelo de Seguridad y Privacidad de la Información MSPI.	A	- Realizar ajustes Plan Estratégico de Seguridad de la Información (PESI) y a la Matriz de aplicabilidad de controles asociados a la NTC 27001 (cuando aplique). - Establecer acciones correctivas, preventivas y de mejora.	- Plan Estratégico de Seguridad de la Información (PESI) y a la Matriz de aplicabilidad de controles asociados a la NTC 27001 ajustados (cuando aplique). - Planes de mejoramiento.	Todos los procesos.
Todos los procesos.	- Información del inventario de activos de información. - Matriz de riesgos de Seguridad de la Información.	P	- Identificar/actualizar los activos de información. - Identificación y/o actualización de riesgos de Seguridad de la Información.	- Registro de activos de información actualizado. - Índice de información clasificada y reservada. - Esquema de Publicación de la Información. - Matriz de riesgos de Seguridad de la Información actualizada.	Todos los procesos.
Proceso de Gestión de Seguridad de la Información.	- Registro de activos de información actualizado. - Índice de información clasificada y reservada.	H	- Tipificar y calificar los activos de información. - Etiquetar los activos de información de acuerdo con el nivel de clasificación.	- Matriz de identificación de riesgos de seguridad y privacidad de la información. - Activos de información etiquetados.	Todos los procesos.
Todos los procesos.	Matriz de identificación de riesgos de seguridad y privacidad de la información.	H	Gestionar los riesgos de seguridad y privacidad de la información.	Riesgos de seguridad y privacidad de la información gestionados.	Proceso de Gestión de la Planeación Institucional.
Todos los Procesos	- Riesgos de seguridad y privacidad de la información identificados. - Activos de información etiquetados.	V	- Realizar monitoreo de los riesgos de seguridad y privacidad de la información. - Evaluar el estado de los activos de información en términos de confidencialidad,	- Informe de monitoreo de los riesgos de seguridad y privacidad de la información. - Informe del estado de los activos de información. - Informe de verificación del	- Todos los procesos. - Alta Dirección.

			integridad y disponibilidad. • Verificar la correcta clasificación y etiquetado de los activos conforme a los lineamientos definidos.	cumplimiento de clasificación y etiquetado de los activos de información.	
1. Proceso de Seguridad de la Información. 2. Proceso de Gestión de Evaluación y Control.	1. Informe de monitoreo de los riesgos de seguridad y privacidad de la información. 1. Informe del estado de los activos de información 1. Informe del etiquetado de los activos de información. 2. Informe de seguimiento a los riesgos de seguridad y privacidad de la información.	A	• Implementar acciones correctivas, preventivas y de mejora sobre la gestión de los activos de información, con base en los resultados del monitoreo y seguimiento. • Actualizar la información clasificada y los mecanismos de control asociados. • Ajustar el mapa de riesgos de seguridad y privacidad de la información de acuerdo con los resultados de evaluación.	• Acciones correctivas, preventivas y de mejora. • Activos de información actualizados. • Mapa de riesgos de seguridad y privacidad de la información actualizado.	Todos los procesos.
1. Todos los procesos. 2. Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC u Organismos de seguridad.	1. Necesidades asociadas a la seguridad y privacidad de la información. 1. Reporte de eventos de seguridad y privacidad de la información. 2. Información de posibles amenazas de seguridad de la información o seguridad digital.	P	Analizar las necesidades, los eventos y posibles amenazas de seguridad y privacidad de la Información.	• Necesidades, eventos y posibles amenazas de seguridad y privacidad de la información analizadas. • Incidentes de seguridad y privacidad de la información.	Todos procesos.
Proceso de Gestión de Seguridad de la Información.	• Necesidades, eventos y posibles amenazas de seguridad y privacidad de la información analizadas. • Incidentes de seguridad y privacidad de la información.	H	• Gestionar las necesidades e incidentes de seguridad y privacidad de la información. • Actualizar el mapa de riesgos de seguridad y privacidad de la información.	• Necesidades seguridad y privacidad de la información gestionadas. • Incidentes de seguridad y privacidad de la información gestionados. • Mapa de riesgos de seguridad y privacidad de la información actualizado.	Todos los procesos.
Proceso de Gestión de Seguridad de la Información.	• Necesidades asociadas a la seguridad y	V	• Verificar la remediación a las necesidades e	Resultados de la verificación y evaluación de las	Proceso de Gestión de Seguridad de la Información.

	privacidad de la información gestionadas. - Incidentes de seguridad y privacidad de la información gestionados. - Mapa de riesgos de seguridad y privacidad de la información actualizado.		incidentes de seguridad y privacidad de la información y la efectividad de los controles implementados. Evaluar los nuevos controles de seguridad y privacidad de la información aplicados y la eficacia de las acciones implementadas para el tratamiento de los riesgos de seguridad y privacidad de la información.	necesidades, incidentes gestionados y eficacia de las acciones tomadas.	
Proceso de Gestión de Seguridad de la Información.	Resultados de la verificación y evaluación de las necesidades, incidentes gestionados y eficacia de las acciones tomadas.	A	- Implementar acciones correctivas, preventivas y de mejora derivadas de los resultados. - Optimizar los controles de seguridad y privacidad de la información con base en los resultados obtenidos.	- Acciones correctivas, preventivas y de mejora implementadas. - Controles de seguridad y privacidad de la información optimizados.	Todos los procesos.

RECURSOS / INSUMOS	PROCESOS INTER-RELACIONADOS	RIESGOS DEL PROCESO
Véase procedimientos del proceso.	Gestión de la Planeación Institucional. Gestión de la Comunicación. Administración del Sistema Integrado de Gestión. Gestión del Servicio Pericial. Gestión de Certificación de Peritos Forenses. Gestión del Conocimiento Científico Forense. Gestión Administrativa. Gestión Financiera. Gestión de Infraestructura Tecnológica y Servicios Informáticos. Gestión del Talento Humano. Gestión y Soporte Jurídico. Gestión de la Seguridad y Salud en el Trabajo. Gestión Ambiental. Gestión Contractual Gestión del Sistema de Evaluación y Control. Gestión del Relacionamento con la Ciudadanía. Gestión de Datos e Innovación.	Véase Mapa de Riesgos Institucional.

PROCEDIMIENTOS Y DOCUMENTOS ASOCIADOS

- [Ver Listado maestro de documentos.](#)

INDICADORES

% de activos de información con controles implementados
Nivel de implementación de estrategias socializadas para fortalecer la cultura de seguridad y privacidad de la información
Nivel de implementación del SGSI
Nivel de incidentes gestionados que comprometieron la disponibilidad, confidencialidad, integridad y privacidad de la información
Nivel de riesgos de seguridad de la información gestionados

VERSIÓN	ELABORACIÓN O MODIFICACIÓN		REVISIÓN		APROBACIÓN		MODIFICACIÓN
	NOMBRE	FECHA	NOMBRE	FECHA	NOMBRE	FECHA	
1	HENRY CORTES CONTRERAS	03/Jul/2026	GEOVANNY GOMEZ OROZCO SONIA PATRICIA CASTANEDA NEIRA	02/Sep/2026	ARIEL EMILIO CORTÉS MARTÍNEZ	11/Sep/2026	No Aplica.

ELABORÓ Ó MODIFICÓ ESTA VERSIÓN	REVISÓ ESTA VERSIÓN	APROBÓ ESTA VERSIÓN
Nombre: HENRY CORTES CONTRERAS Cargo: Profesional Especializado Fecha: 27/Ago/2026	Nombre: OLGA LUCIA GARCIA TORRES Cargo: Profesional Especializado Fecha: 28/Ago/2026 Nombre: GEOVANNY GOMEZ OROZCO Cargo: PROFESIONAL ESPECIALIZADO Fecha: 31/Ago/2026 Nombre: SONIA PATRICIA CASTANEDA NEIRA Cargo: Coordinador Fecha: 02/Sep/2026	Nombre: ARIEL EMILIO CORTÉS MARTÍNEZ Cargo: DIRECTOR GENERAL Fecha: 11/Sep/2026