En el marco del Modelo de Seguridad y Privacidad de la Información y teniendo en cuenta los lineamientos para la Administración del Riesgo - (L-DE-01) de la Presidencia de la República, se describen los riesgos del Sistema de Gestión de la Seguridad de la Información- SGSI, que pueden afectar la disponibilidad, integridad y confidencialidad de los activos de información.

Con la identificación anticipada de los riesgos de la contratación lo que se pretende es básicamente conocer cuáles serían las potenciales situaciones que, de acuerdo a cada contratación, podrían afectar su normal desarrollo y en tal sentido, encontrar a quien corresponde asumirlo, identificando además el tratamiento y las medidas de prevención o mitigación.

Si se considera que algunos de los riesgos que se encuentran en la siguiente matriz-SGSI aplican para el desarrollo del proceso de contratación que requiere adelantar, el usuario deberá incluirlos en la matriz respectiva.

MATRIZ DE RIESGOS
Sistema de Gestión de la Seguridad de la Información - SGSI

No.	Nombre del Riesgo	Descripción del Riesgo	Clase de riesgo	Causas	Efectos	Probabilidad	Impacto	Controles
1	Posibilidad de afectación reputacional, por la pérdida de disponibilidad de los servicios TIC, debido a la falta de seguimiento y monitoreo de las	Corresponde a los servicios que hacen parte de la Oficina de Tecnologías y Sistemas de Información, que puedan estar no disponibles.	SGSI	Mala identificación de los requisitos técnicos y funcionales	Indisponibilidad de los servicios de TIC	Alta	Mayor	Aplicar el procedimiento de control de cambios
				Errores humanos	Violación a las políticas de seguridad			Implementar actualizaciones de las diferentes aplicaciones utilizadas en la Entidad

No.	Nombre del Riesgo	Descripción del Riesgo	Clase de riesgo	Causas	Efectos	Probabilidad	Impacto	Controles
	herramientas TIC - SGSI			No cumplimiento del procedimiento establecido	Pérdida de imagen			Monitorear los servicios tecnológicos
				Error en la manipulación de la Plataforma Tecnológica	Quejas, reclamos frente a la prestación de servicios			Realizar la entrega de Rol con las respectivas actividades
				Dualidad de tareas en los funcionarios				Ejecutar pruebas de los servicios tecnológicos replicados en el centro alterno
				No activación de registros de logs				
				Error en las configuraciones de los controles				
				Deficiencias en cultura de la seguridad de la información e Informática	Retrasos en los procesos de los funcionarios y contratistas			Utilizar la herramienta de prevención de perdida de información (DLP)
				Fallas Técnicas de Hardware	Problemas de Seguridad Nacional (perdida de Información reservada)			Emplear la Autenticación de dos factores
				Conflicto Armado	Afectación derechos a titulares de datos personales			Aplicar Cifrado de Información pública clasificada y pública reservada
				Vandalismo Informático	Sanciones legales y disciplinarias			Realizar la verificación de vulnerabilidades de la plataforma TIC
				Desconocimiento del manual de políticas de seguridad.	Afectación de la imagen de la Entidad			Mantener operativas las herramientas tecnológicas

No.	Nombre del Riesgo	Descripción del Riesgo	Clase de riesgo	Causas	Efectos	Probabilidad	Impacto	Controles
2	Posibilidad de afectación reputacional, por la pérdida de la documentación pública reservada y publica clasificada, o identificable de carácter personal (datos personales) que se encuentra en la Plataforma de TI o repositorios físicos, debido a accesos no autorizados - SGSI	En caso de que se presente perdida de información pública reservada o pública clasificada, o de carácter privado (información identificable como personal - datos personales) puede ocasionar afectación en la imagen de la Entidad.	Tecnología	Usuarios inconformes que puedan atentar contra la seguridad de la información		Media	Mayor	Realizar la entrega de Rol con las respectivas actividades
				Falta de conocimiento técnico en el personal que administra la plataforma informática o la información.				Ejecutar los procedimientos de backups, configuración de SAN
				Gestión de vulnerabilidades de la plataforma				Monitorear las herramientas de seguridad de la información
				Errores Humanos				Aplicar Políticas de Seguridad de la información
				Ataques cibernéticos y delitos informáticos				Utilizar contraseñas seguras.
				Obsolescencia de la plataforma				
				Deficiencias en definición, aplicación o seguimiento de las políticas de seguridad				
				Dualidad de tareas en los funcionarios				
				Deficiencias en el procedimiento de Borrado Seguro				
				Pérdida de equipos tecnológicos con información contenida				

No.	Nombre del Riesgo	Descripción del Riesgo	Clase de riesgo	Causas	Efectos	Probabilidad	Impacto	Controles
3	Posibilidad de afectación reputacional, por pérdida de la gestión de la continuidad del negocio en activos de información, debido a situaciones adversas - SGSI	La Entidad puede ser afectada por no disponer de una gestión de la continuidad del negocio al no tener la prestación de sus servicios, por situaciones adversas.	SGSI	Fallas en los equipos tecnológicos	Afectación de la Imagen de la Entidad	baja	Mayor	Realizar pruebas de disponibilidad y continuidad para los servicios que proporciona la Entidad.
				Falta de Mantenimientos preventivos	Retrasos en los procesos de los funcionarios			Aplicar los cambios a los sistemas mediante el uso de procedimientos formales de control de cambios.
				Desconocimiento del manual de políticas de seguridad	Retrasos en los procesos de los contratistas			Actualizar la documentación para la continuidad de la seguridad de la información.
				Equipos desactualizados	Problemas de Seguridad Nacional (pérdida de Información reservada)			
					Pérdida de credibilidad de las herramientas informáticas			
					Sanciones legales y disciplinarias			
					Retrasos en los procesos de los funcionarios			
				Deficiencias en el procedimiento de Borrado Seguro	Retrasos en los procesos de los funcionarios y contratistas	media	catastrófico	Aplicar el procedimiento de borrado seguro para equipos.

No.	Nombre del Riesgo	Descripción del Riesgo	Clase de riesgo	Causas	Efectos	Probabilidad	Impacto	Controles
4	Posibilidad de afectación reputacional, por el uso indebido de la información pública clasificada y/o pública reservada de la Entidad, así como de aquella identificable de carácter personal (datos personales), debido a la falta de controles para la protección de la información -SGSI	La información activa o cuando ha dejado de utilizarse debe gestionarse de una forma segura, porque la información clasificada o reservada, así como aquella identificable de carácter personal (datos personales) contenida en medios digitales o físicos (hojas de papel, carpetas, folletos, dispositivos de almacenamiento - memoria USB, disco duro - , medios magnéticos y ópticos) puede ser manipulada o utilizada por delincuentes para aprovechar su contenido con fines distintos a la finalidad de dicha información (sea organizacional o personal) y afectar la imagen de la Entidad.	SGSI	Pérdida de equipos tecnológicos con información contenida.	Problemas de Seguridad Nacional (perdida de Información reservada)			Realizar la eliminación de documentos de archivo de acuerdo al procedimiento establecido por la Entidad.
				Desconocimiento de Baja de Bienes	Afectación derechos a titulares de datos personales			Utilizar la criptografía para mantener protegida información
				Desconocimiento del manual de políticas de seguridad	Sanciones legales y disciplinarias			Proteger la información mediante políticas y procedimientos de la Seguridad de la Información
				Deficiencias en cultura de la seguridad de la información e Informática	Afectación de la imagen de la Entidad			
				Desconocimiento procedimiento de eliminación de Documentos				
				Ataques cibernéticos y delitos informáticos	Afectación de la Imagen de la Entidad	Muy Alta	Catastrófico	Gestionar las vulnerabilidades técnicas
				Falta de conocimiento técnico en el personal que administra la plataforma informática	Retrasos en los procesos de los funcionarios			Aplicar la seguridad de servicios de las aplicaciones en redes públicas.
				Falta de Verificación de vulnerabilidades de la plataforma TIC	Retrasos en los procesos de los contratistas			Proteger los activos de información contra los códigos maliciosos
				Obsolescencia de la plataforma	Problemas de Seguridad Nacional (pérdida de			Realizar la separación de redes

No.	Nombre del Riesgo	Descripción del Riesgo	Clase de riesgo	Causas	Efectos	Probabilidad	Impacto	Controles
5	Posibilidad de afectación reputacional, por hurto, perdida o fuga de información, debido a ataques cibernéticos - SGSI	Los ataques cibernéticos se pueden presentar en la Entidad ocasionados por personas malintencionadas (ciberatacantes), afectando sistemas de información, aplicativos informáticos, páginas Web, equipos de cómputo, servidores que contienen y procesan información, comprometiendo la Confidencialidad, Integridad y Disponibilidad de la información.	SGSI		Información reservada)			
				Desconocimiento Manual de políticas de Seguridad de la Información	Pérdida de credibilidad de las herramientas informáticas			Utilizar Perímetros de Seguridad Física
					Sanciones legales y disciplinarias			Restringir el acceso a código fuente de Programas evitar cambios involuntarios.
								Utilizar contraseñas seguras
								Revisar la configuración y afinamiento de las herramientas de seguridad informática.
								Contener el Ataque Cibernético
6	Posibilidad de afectación reputacional por la pérdida de documentos de archivo debido a la inadecuada aplicación de los procesos archivísticos y de conservación en los archivos de LA PRESIDENCIA DE LA REPÚBLICA - SGSI	La pérdida de documentos de archivo se da por su extravío, hurto o por daño irremediable al soporte en que se encuentran lo que tiene como consecuencia que la información contenida en los archivos afectados no se pueda recuperar, de manera que la Entidad no tiene capacidad para disponer de los datos suficientes para la toma de decisiones basadas en antecedentes, para uso de la administración en el servicio al ciudadano y como fuente de la historia. Adicionalmente, el incumplimiento en la normatividad	SGSI	Espacios físicos y mobiliario que no cumplen con los requisitos técnicos y de seguridad para la conservación y custodia de los archivos	Hallazgos en auditorías interna o externas, o en visita de inspección y vigilancia del Archivo General de la Nación	Alta	Catastrófico	Realizar seguimiento a préstamos y consulta de expedientes de archivo
				Deficiencias en el diligenciamiento y actualización del inventario documental	Pérdida total o parcial del patrimonio documental de la Entidad y de la información contenida en los soportes documentales			Identificar el estado de los archivos de gestión
				Actos vandálicos y terrorismo, desastres naturales, presencia de humedad, deficiencias en la iluminación y/o ventilación, acción causada por la presencia de insectos, bacterias, hongos o roedores.	Afectación en la salud de los funcionarios que acceden a los documentos de archivo			Realizar seguimiento a Inventarios documentales

No.	Nombre del Riesgo	Descripción del Riesgo	Clase de riesgo	Causas	Efectos	Probabilidad	Impacto	Controles
		archivística, expone LA PRESIDENCIA DE LA REPÚBLICA a sanciones según lo establece la Ley 594 de 2000 en el artículo 35.						
				Manipulación constante, inadecuada o sin protección de los soportes documentales físicos	Sanciones disciplinarias, penales o fiscales, demandas o acciones judiciales contra la Entidad			Sensibilizar y orientar a los servidores del LA PRESIDENCIA DE LA REPÚBLICA en temas de gestión documental y manejo de archivos
				No aplicación de los procesos de organización de los documentos de archivo (clasificación, ordenación y descripción) por desconocimiento de la normatividad archivística para su conservación y preservación	Vulneración de derechos de personas naturales o jurídicas o afectación de intereses públicos por la falta de oportunidad, calidad o veracidad en la respuesta a solicitudes de información de usuarios internos o externos			Mantener las condiciones ambientales y de infraestructura de los archivos
				Fallas en la aplicación de controles de acceso, consulta y reintegro de los documentos de archivo.	Afectación a la imagen institucional			
7	Posibilidad de pérdida reputacional por toma de decisiones erradas debido a la deficiencia de la información reflejada en los estados financieros - SGSI	La Entidad puede llegar a tomar malas decisiones que afectan la transparencia y su misionalidad por la información errada que pueda llegar a reflejar los estados financieros.	Financiero	Falta de identificación de políticas contables para el reconocimiento, medición revelación y presentación de los hechos económicos o aplicación de políticas contables que desborden lo establecido en Régimen de Contabilidad Pública o que no son permitidas por este para el reconocimiento, medición revelación y presentación de los hechos económicos del LA PRESIDENCIA DE LA REPÚBLICA	Opinión negativa, adversa o abstención a los Estados Financieros de la Entidad, por parte de la Contraloría General de la República.	Baja	Mayor	Realizar seguimiento al cumplimiento de las Políticas Contables.

No.	Nombre del Riesgo	Descripción del Riesgo	Clase de riesgo	Causas	Efectos	Probabilidad	Impacto	Controles
				Ausencia de un procedimiento mediante el cual todos los hechos económicos ocurridos en cualquier dependencia de la Entidad sean informados y soportados de manera oportuna al Grupo de Contabilidad.	Hallazgos por auditorías internas y externas			Contar con el Manual de Políticas contables teniendo en cuenta la normatividad vigente y aplicable al LA PRESIDENCIA DE LA REPÚBLICA
				Carencia de políticas o procedimientos para realizar las conciliaciones, cruces de información y tomas físicas que garanticen el registro físico y contable de los activos, pasivos, ingresos y gastos.	Sanciones disciplinarias			Contar con Políticas y procedimientos para realizar las conciliaciones, cruces de información y tomas físicas.
				Falta de un comité técnico de sostenibilidad contables que propenda por la depuración contable permanente y sostenible de la calidad de la información	Inadecuada toma de decisiones por parte de los usuarios de los Estados Financieros			Realizar el Comité Técnico de Sostenibilidad Contable cuando se requiera
				Ocurrencia de hechos económicos no considerados en el Régimen de Contabilidad Pública ni definidos en la doctrina contable pública				Realizar el manejo y Control Administrativo de los Bienes de Propiedad del LA PRESIDENCIA DE LA REPÚBLICA.
				Desconocimiento y/o desactualización de la normatividad vigente. Interpretación errónea del hecho económico de acuerdo con el marco normativo				Impartir directrices en materia contable a los funcionarios del Grupo de Contabilidad y al Contador del Fondo Cuenta. Participar en las capacitaciones dadas por la Contaduría General de la Nación y el SIIF Nación.
				Error en la parametrización del aplicativo y/o Deficiencia de tipo tecnológico en el aplicativo SIIF				Cumplir con lo establecido en el procedimiento para la elaboración de los Estados Financieros de la Presidencia de la República P-GF-07.

No.	Nombre del Riesgo	Descripción del Riesgo	Clase de riesgo	Causas	Efectos	Probabilidad	Impacto	Controles
				Falta de planificación para el registro, consolidación y elaboración de informes de los hechos económicos desarrollados por la Entidad. Registros globales de hechos económicos.				Realizar las conciliaciones de los saldos contables frente a los valores reportados por las diferentes dependencias que participan en el proceso contable.
				Utilización inadecuada de cuentas y subcuentas y/o No registrar oportunamente la información.				Programar las fechas para entregar la información por parte de los responsables para su elaboración y consolidación.
				No envío oportuno de la información al Grupo de Contabilidad, o que esta no cuente con los soportes necesarios para realizar los registros contables, por parte de las diferentes dependencias del LA PRESIDENCIA DE LA REPÚBLICA.				Reexpresar Estados Financieros.
				Registro de hechos económicos por un valor diferente al correcto o sin sus respectivos soportes.				
				No realizar el backup de los aplicativos internos de almacén ALADINO y de nómina KACTUS.				