Presidencia	ESTUDIOS PREVIOS PARA CONTRATACIÓN DIRECTA

1. DESCRIPCIÓN Y JUSTIFICACIÓN DE LA NECESIDAD:

El artículo 36 del Decreto No. 2647 de 2022, establece entre otras las funciones de la Oficina de Tecnologías y Sistemas de Información del Departamento Administrativo de la Presidencia de la República, señalando:

(…)

12. Prestar el soporte técnico básico o de primer nivel a los usuarios internos del Departamento garantizando el adecuado funcionamiento de la infraestructura tecnológica base. (…)"

Siguiendo con la normativa aplicable, el artículo 38 de la Resolución 0163 del 23 de febrero de 2023 establece entre otras las siguientes funciones a cargo del Grupo de Soporte de Tl y Mesa de Ayuda de la Oficina de Tecnologías y Sistemas de Información del Departamento Administrativo de la Presidencia de la República, señalando:

(…)

1. Participar en la elaboración del plan estratégico, plan de acción, plan anual de adquisiciones, indicadores de gestión y mapa de riesgos asociados con la gestión de la dependencia.

(…)

5. Realizar las actividades necesarias para garantizar la disponibilidad de los servicios tecnológicos del portafolio que soportan la operación dando cumplimiento a la política de seguridad de la información.

(…)

11. Adelantar los trámites necesarios para la adquisición, mantenimiento de los bienes de tecnología informática requeridos por la entidad, atendiendo el proceso contractual de acuerdo con la normatividad vigente y las políticas de la entidad.

(…)

A su turno, la Entidad implementó un sistema que permite gestionar la información de registro de ingreso y salida de visitantes y funcionarios de las diferentes sedes del DAPRE, el cual se encuentra integrado por el software **MF ENTERPRISE**, Molinetes, Lectoras faciales, Lectoras de huella, Cámaras de video USB, Scanner de documentos, etc.

Así pues, varios de los equipos actualmente instalados han cumplido su vida útil y presentan reiteradas fallas en sus mecanismos, la consecución de los repuestos para su reemplazo, se hace costosa y difícil de conseguir debido a su obsolescencia, por lo cual se requiere realizar la actualización en algunos de sus componentes, así como la adquisición de elementos que se puedan integrar con la solución actual para fortalecer los mecanismos de seguridad y control de acceso en la instalaciones de la Entidad.

Los principales componentes que se requieren actualizar son:

1. Actualización del molinete existente de control de ingreso peatonal en la sede de Casa Galán bajada al parqueadero.
2. Actualización de las unidades biométricas MF-PRO de registro y control de acceso asociadas a los centros de cableados de la Entidad.

Esta intervención, busca integrar dichos puntos al sistema de control de acceso actualmente implementado en el Departamento Administrativo de la Presidencia de la República, permitiendo centralizar de forma, segura y eficiente el ingreso de funcionarios, contratistas y visitantes.

Actualmente, el control de acceso de la sede Galán cuenta con un molinete de tipo mecánico, el cual presenta deficiencias en su funcionamiento y bloqueos constantes, así como desajustes internos debido al modelo del equipo, lo que repercute en la imposibilidad de invertir en su mantenimiento o actualización, ya que no existe disponibilidad de repuestos en el mercado.

Asimismo, las lectoras MF-Pro instaladas en los centros de cableado que operan mediante lectura de huella digital, han mostrado deterioro tras más de 12 años de uso continuo. Estas fallas afectan

directamente el correcto funcionamiento del sistema de control de acceso incidiendo en errores estadísticos de ingreso.

Adicionalmente, dichas lectoras presentan limitaciones en sus actualizaciones, ya que el fabricante ha dejado de liberar nuevas versiones de software para este modelo. En caso de fallas, no existen repuestos disponibles en el mercado que permitan su reparación, lo cual representa un riesgo operativo, dado que, de dañarse, no sería posible restablecer su funcionamiento.

La actualización contribuirá a la mitigación de riesgos relacionados con acceso a personal no autorizado a los centros de cableado. Asimismo, facilitará una individualización rápida y precisa de las personas que acceden a las instalaciones, optimizando los tiempos de registro y fortaleciendo los protocolos de seguridad.

Los avances tecnológicos recientes han permitido el desarrollo de unidades de identificación facial **compatibles con la plataforma MF Enterprise**, las cuales ofrecen una experiencia mejorada para los usuarios. Estas unidades permiten la identificación mediante lectura facial, reduciendo los tiempos de ingreso y asegurando una integración efectiva con las bases de datos institucionales.

La incorporación de estos elementos y componentes al sistema actual de control de acceso garantiza su correcto funcionamiento, ampliando su cobertura y robusteciendo su capacidad operativa.

Adicionalmente, se busca implementar un mecanismo de doble autenticación en los centros de cableado, con el fin de reforzar los niveles de seguridad en áreas críticas de la Entidad. Esta medida permitiría validar la identidad de los funcionarios y contratistas mediante un segundo factor de verificación, complementario a la identificación facial, lo cual contribuiría a prevenir accesos no autorizados y garantizar la trazabilidad de los ingresos a zonas sensibles, alineándose con las mejores prácticas en seguridad tecnológica y física.

Cabe destacar que la empresa **SERVICIO DE TECNOLOGÍA Y COMUNICACIONES FENIX S.A.S sigla: STC FENIX S.A.S.,** posee los derechos patrimoniales del sistema de control de acceso implementado en las diferentes sedes de la Entidad, lo que la convierte en el proveedor idóneo para el suministro y configuración de los elementos requeridos para esta actualización.

Finalmente, dicha empresa ha aportado la Certificación de Registro de Soporte Lógico, Libro 11, Tomo 142, Partida 388, con fecha del 19 de julio de 2021, emitida por el Ministerio del Interior y de Justicia – Dirección Nacional de Derechos de Autor, en la cual se establece que el titular del derecho patrimonial de la obra "MF ENTERPRISSE" es **SERVICIO DE TECNOLOGÍA Y COMUNICACIONES FENIX S.A.S sigla: STC FENIX S.A.S**.

2. OBJETO Y ESPECIFICACIONES TÉCNICAS:

OBJETO: Modernizar el sistema de control de acceso en los centros de cableado y en la entrada al parqueadero Galán, en cumplimiento de las especificaciones técnicas establecidas.

ESPECIFICACIONES TÉCNICAS:

Cantidad	Referencia	Suministro de Tecnología Control de Acceso Renovación Tecnológica MF PRO
24	MFACE7-PRO-MIN	MFACE7-PROMIN-Lector Facial FACE-7 PROMIN - Lector de Acceso Multitecnología - IP65, IPS HD 7" Facial, Tarjeta, Montaje Interiores de Baja Exposición. Centros de cableado **NOTA 1:** Las presentes actualizaciones tecnológicas no implican instalaciones ya que se hace uso de la infraestructura instalada, es decir se cotiza bajo la premisa de los mismos lugares de operación actual.
2	TSS-309L15060	Pasillo de Acceso Lateral 1500*120*980 Pass de 60

3. MODALIDAD DE SELECCIÓN:

La Entidad acudirá a la modalidad de selección de Contratación Directa prevista en el numeral 4 del artículo 2ª de la Ley 1150 de 2007.

- Contratos o Convenios Interadministrativos. (Literal c del numeral 4 del artículo 2 de la Ley 1150 de 2007). (__)
- **Inexistencia de Pluralidad de Oferentes. (Literal g del numeral 4 del artículo 2 de la Ley 1150 de 2007). (_X_).**
- Arrendamiento y Adquisición de Inmuebles. (Literal i del numeral 4 del artículo 2 de la Ley 1150 de 2007). (__).
- Cabildos Indígenas y Asociaciones de Autoridades Tradicionales Indígenas. (Literal l del numeral 4 del artículo 2 de la Ley 1150 de 2007). (__)
- Consejos Comunitarios de las Comunidades Negras, regulados por la ley 70 de 1993. (Literal m del numeral 4 del artículo 2 de la Ley 1150 de 2007). (__)
- Organizaciones de base de personas pertenecientes a poblaciones afrocolombianas, raizales y Palenqueras o con las demás formas y expresiones organizativas. (Literal n del numeral 4 del artículo 2 de la Ley 1150 de 2007). (__)

En virtud de la modalidad de contratación indicada, los factores objeto de verificación corresponden a la condición de proveedor exclusivo para la **Solución MF Enterprise**, los cuales se acreditan para la presente contratación teniendo en cuenta que la empresa **SERVICIO DE TECNOLOGÍA Y COMUNICACIONES FENIX S.A.S sigla: STC FENIX S.A.S.,** mediante documento adjunto, emitido por la Dirección Nacional de Derechos de Autor, es la propietaria del software MF ENTERPRISE y tiene la titularidad de los derechos de autor sobre dicho software.

El futuro contratista aportó la "Certificación de Registro de Soporte Lógico", Libro 11 Tomo 142 Partida 388 fechado el 19 de julio de 2021, emitida por el Ministerio del Interior y de Justicia – Dirección Nacional de Derechos de Autor, en la cual establece que el titular del derecho patrimonial de la obra "MF ENTERPRISSE" es **SERVICIO DE TECNOLOGÍA Y COMUNICACIONES FENIX S.A.S sigla: STC FENIX S.A.S.**

Dado que la sociedad **SERVICIO DE TECNOLOGÍA Y COMUNICACIONES FENIX S.A.S sigla: STC FENIX S.A.S**. cuenta con los Derechos Patrimoniales del sistema de control de acceso ubicado en las diferentes sedes de la Entidad, es en consecuencia la empresa idónea para suministrar y configurar los elementos y componentes necesarios para ampliar la cobertura requerida, de acuerdo con la necesidad de la Entidad.

Sumado a lo anterior, la sociedad propietaria, manifiesta que no cuenta con distribuidores, intermediarios o ningún tercero para la venta, suministro o implementación la solución, somos los únicos con el personal especializado y capacitado para desarrollar, suministrar, programar y hacer mantenimiento al Sistema.

OTROS BENEFICIOS:

- **COMPATIBILIDAD E INTEGRACIÓN**: El proveedor cuenta con el conocimiento especializado y la capacidad técnica para suministrar equipos y componentes totalmente compatibles con el software MF ENTERPRISE y el resto de los dispositivos existentes, asegurando una integración eficiente sin poner en riesgo la funcionalidad del sistema.
- **GARANTÍA Y SOPORTE TÉCNICO:** Al trabajar con un proveedor exclusivo, se garantiza el acceso a soporte técnico especializado, repuestos originales y actualizaciones de software, lo que reduce el riesgo de incompatibilidades y facilita la solución de problemas de manera ágil y efectiva.
- **OPTIMIZACIÓN DE COSTOS Y TIEMPOS:** La adquisición de equipos y repuestos a través de un proveedor exclusivo permite optimizar los costos derivados de la búsqueda de componentes en el mercado, evitando gastos excesivos y retrasos generados por la escasez de los mismos y la obsolescencia de los equipos.
- **CONTINUIDAD OPERATIVA:** Mantener la relación con un proveedor que domina la tecnología instalada asegura la continuidad de los procesos de seguridad y control de acceso, minimizando riesgos y garantizando la protección de las instalaciones.

- **SIMPLIFICACIÓN DE PROCESOS**: Coordinación con el proveedor, reduciendo costos administrativos y tiempo, en colaboración, comunicación y mejora continua, optimizando la cadena de equipos requeridos.
- **CALIDAD Y CONSISTENCIA**: Mayor control sobre los estándares de calidad al trabajar con una sola fuente.
- **RELACIONES SÓLIDAS**: Fomenta la colaboración, comunicación y mejora continua, optimizando la cadena de suministro.
- **SERVICIO PRIORITARIO**: Posibilidad de recibir mejor atención y servicio al cliente.

NOMBRE O RAZÓN SOCIAL DEL FUTURO CONTRATISTA: SERVICIO DE TECNOLOGÍA Y COMUNICACIONES FENIX S.A.S sigla: STC FENIX S.A.S., identificado con NIT No. 901475652-9.

4. OBLIGACIONES ESPECÍFICAS DEL FUTURO CONTRATISTA: El futuro contratista se obliga a:

1. Entregar y configurar los bienes de acuerdo con las especificaciones técnicas establecidas y la propuesta presentada.
2. Emplear personal idóneo, calificado y debidamente autorizado e identificado para la ejecución del objeto contractual, previa autorización por parte del supervisor del contrato.
3. Responder por los daños que puedan causarse a **LA ENTIDAD** durante la configuración de los bienes objeto del contrato.
4. Entregar los bienes objeto del contrato, con la última actualización tecnológica en el hardware y/o software que forma parte de la solución propuesta.

GARANTÍA: **EL CONTRATISTA** mantendrá durante los doce (12) meses siguientes a la entrega de los bienes, la garantía de los elementos descritos en la oferta económica.

5. VALOR ESTIMADO DEL CONTRATO Y SU JUSTIFICACIÓN:

El valor del contrato será hasta por la suma de **CIENTO CINCUENTA Y SIETE MILLONES TRESCIENTOS OCHENTA Y TRES MIL OCHOCIENTOS CATORCE PESOS MONEDA LEGAL ($157.383.814),** incluidos todos los impuestos, gastos, y costos directos e indirectos que se requieran para la ejecución del contrato, así:

Cantidad	Referencia	Suministro de Tecnología Control de Acceso Renovación Tecnológica MF PRO	Valor Unitario	Valor Total
24	MFACE7-PRO-MIN	MFACE7-PROMIN-Lector Facial FACE-7 PROMIN - Lector de Acceso Multitecnología - IP65, IPS HD 7" Facial, Tarjeta, Montaje Interiores de Baja Exposición. Centros de cableado **NOTA 1:** Las presentes actualizaciones tecnológicas no implican instalaciones ya que se hace uso de la infraestructura instalada, es decir se cotiza bajo la premisa de los mismos lugares de operación actual.	$ 4.191.286	$ 100.590.864
2	TSS-309L15060	Pasillo de Acceso Lateral 1500*120*980 Pass de 60	$ 15.832.221	$ 31.664.442
			Sub total	$ 132.255.306
			IVA	$ 25.128.508
			Total propuesta	**$157.383.814**

6. RUBRO PRESUPUESTAL:

INFORMACIÓN DEL PAA	RUBRO Y CÓDIGOS CERTIFICADOS
CERTIFICACIÓN PAA	Programado en el PAA
RUBRO PRESUPUESTAL	**No.** A-02-02-02-008-007 **FUNCIONAMIENTO: X ó INVERSIÓN: ___** **No. RUBRO PRESUPUESTAL DESAGREGADO (Inversión):** N/A
CÓDIGO (S) DE CLASIFICACIÓN DE BIENES Y SERVICIOS	72151701
CÓDIGO BPIN	N/A

7. FORMA DE PAGO DEL CONTRATO:

El valor del contrato se pagará a través de la pagaduría de la Entidad contra facturación presentada por parte el contratista, con base en los bienes entregados, instalados y configurados a satisfacción, previo cumplimiento de los siguientes requisitos:

a) Certificación expedida por el representante legal del contratista o su revisor fiscal, según corresponda, donde se acredite estar a paz y salvo por concepto del pago de sus obligaciones a los Sistemas de Salud, Riesgos Laborales, Pensiones y Aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje.
b) Certificación emitida por el supervisor del contrato respecto de la entrega, configuración y recibo a satisfacción de los bienes.
c) Certificado de ingreso al almacén por el Grupo de Recursos Físicos del Área Administrativa de los bienes objeto del contrato.
d) Trámite de la cuenta respectiva.

NOTA UNP: No obstante, la forma de pago prevista, ésta queda sujeta a la situación de los recursos por parte del Ministerio de Hacienda y Crédito Público, una vez se encuentre aprobado el **PAC** (Programa Anual Mensualizado de Caja).

NOTA DOS: LA ENTIDAD pagará a **EL CONTRATISTA,** dentro de los diez (10) días hábiles siguientes a la radicación de los documentos por parte del supervisor del contrato en el Área Financiera de **LA ENTIDAD**.

NOTA TRES: Si la factura o cuenta de cobro no ha sido correctamente elaborada o no se acompañan los documentos requeridos para el pago y/o se presentan de manera incorrecta, el término para éste sólo empezará a contarse desde la fecha en que se aporte el último de los documentos y/o se presenten en debida forma. Las demoras que se presenten por estos conceptos, serán responsabilidad de **EL CONTRATISTA** y no tendrán por ello derecho al pago de intereses o compensación de ninguna naturaleza**.**

NOTA CUATRO: Cuando a ello hubiere lugar, presentar como requisito necesario para el pago, la factura electrónica validada previamente por la DIAN conforme la Directiva Presidencial No. 09 del 17 de septiembre de 2020 y la Resolución No.042 del 05 de mayo de 2020, modificada parcialmente por la Resolución No.094 del 30 de septiembre de 2020, y dar cumplimiento a lo establecido en la circular publicada en la página WEB de **LA ENTIDAD** https://dapre.presidencia.gov.co/normativa/normativa/CIR21-00000022 IDM.pdf**.**

NOTA CINCO: Al pago se le efectuarán los respectivos descuentos por impuestos de ley y las contribuciones respectivas.

NOTA SEIS: El procedimiento para el pago podrá modificarse de conformidad con el trámite de la factura electrónica en el SIIF Nación.

8. ANÁLISIS DE GARANTÍAS A REQUERIR:

Para avalar el cumplimiento idóneo y oportuno de las obligaciones estipuladas, el pago de las multas, de la pena pecuniaria y demás sanciones que, dado el caso, pudieren imponerse, EL CONTRATISTA deberá prestar una garantía única, consistente en póliza expedida por una compañía de seguros legalmente autorizada para funcionar en Colombia a favor de la NACIÓN Y/O EL DEPARTAMENTO

ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPÚBLICA, (Nit: 899.999.083-0). Con los siguientes amparos:

i. **CUMPLIMIENTO DEL CONTRATO**: Para garantizar el cumplimiento general del contrato, el monto del amparo será el equivalente al veinte por ciento (20%) del valor total del contrato, con una vigencia igual al plazo del contrato y un (1) año más.
ii. **CALIDAD DEL SERVICIO:** Para garantizar la calidad del servicio, por un valor equivalente al veinte por ciento (20%) del valor del contralo, con una vigencia igual al plazo del contrato y un (1) año más.
iii. **PAGO DE SALARIOS, PRESTACIONES SOCIALES E INDEMNIZACIONES.** Para garantizar el pago de salarios y prestaciones sociales a cargo del Contratista. Por una cuantía equivalente al cinco (5%) del valor total del contrato, con una vigencia igual al plazo de este contrato y tres (3) años más.
iv. **CALIDAD Y CORRECTO FUNCIONAMIENTO DE LOS BIENES:** Para avalar la calidad de los bienes entregados el monto de amparo será el equivalente al veinte por ciento (20%) del valor total de este contrato, con una vigencia igual al plazo del contrato y un (1) año más.

9. PLAZO DE EJECUCIÓN DEL CONTRATO: El plazo de ejecución del contrato será hasta el **31 de diciembre de 2025** previa aprobación de la garantía y registro presupuestal.

10. LUGAR DE EJECUCIÓN, DE ENTREGA O DE PRESTACIÓN DEL SERVICIO:

El lugar para la entrega y configuración de los bienes objeto del contrato será la ciudad de Bogotá D.C., en las diferentes sedes de **LA ENTIDAD**, ubicadas en: calle 7 No. 6-54, carrera 8 No. 7-26, carrera 8A No. 7-57, Casa Equidad, en la calle 10 # 1-15.

PROYECTOS DE INVERSIÓN:

Señale si esta contratación es financiada con recursos de Proyectos de Inversión SI (__) NO (**X**)

11. OTRAS OBSERVACIONES.

DESIGNACIÓN DE SUPERVISIÓN: Se solicita designar como supervisor al Coordinador del Grupo de Soporte de TI y Mesa de Ayuda

ANÁLISIS DEL SECTOR: Se adjunta a este estudio previo el análisis del sector.

ANÁLISIS DEL RIESGO:

Riesgos previsibles que puedan afectar el equilibrio económico del contrato y la asignación de riesgo entre las partes contratantes, de conformidad con el artículo 4 de la Ley 1150 de 2007 se debe incluir la tipificación, estimación (forma de determinar el valor económico exacto del riesgo y asignación

	Clase	Fuente	Etapa	Tipo	Descripción	secuencia de la ocurrencia del evento	Probabilidad	Impacto	Valoración	Categoría	¿A quién se le asigna?	Tratamiento/ Control a ser implementado	Impacto después del tratamiento				¿Afecta la ejecución del contrato?	onsable por implementar el tratamiento	a estimada en que se inicia el tratamiento	stimada en que se completa el tratamiento	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración	Categoría					ómo se realiza el monitoreo?	Periodicidad
1	General	Externo	Ejecución	Operacional	Incumplimiento de las obligaciones por parte del contratista	n inadecuada del objeto del contrato	2	1	3	Bajo	Contratista	Realizar seguimiento periódico al cumplimiento de las obligaciones pactadas en el contrato	1	1	2	Bajo	Sí	Supervisor	Desde el inicio del contrato	sta la terminación del contrato	uimiento al cumplimiento de las obligaciones del contrato	Diariamente

	Clase	Fuente	Etapa	Tipo	Descripción	secuencia de la ocurrencia del evento	Probabilidad	Impacto	Valoración	Categoría	¿A quién se le asigna?	Tratamiento/ Control a ser implementado	Impacto después del tratamiento				¿Afecta la ejecución del contrato?	ponsable por implementar el tratamiento	a estimada en que se inicia el tratamiento	stimada en que se completa el tratamiento	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración	Categoría					ómo se realiza el monitoreo?	Periodicidad
2	General	Externo	Ejecución	Operacional	Deficiencias en la calidad de los servicios prestados	ción deficiente de los servicios convenidos	2	2	4	Bajo	Contratista	Notificar al contratista sobre la deficiencia de los servicios y solicitar la mejoría en la calidad del servicio	1	2	3	Bajo	No	Contratista	Desde el inicio del contrato	Hasta la terminación del contrato	ción de las condiciones de calidad exigidas para la prestación del servicio	Durante la prestación del servicio
3	Específico	Externo	Planeación	Financiero	Variación de la TRM cuando sea un producto importado	Desequilibrio económico del contrato	3 Posible	3. Moderado	6	Alto	Contratista	Aceptar el Riesgo. No puede ser evitado ni ser transferido o el costo de evitarlo o transferirlo es muy alto. En este caso se recomienda al contratista tomar medidas para reducir el Riesgo o mitigar su impacto, como son: la adquisición de suficientes existencias para la atención del Contrato, planeación acorde con las necesidades de la Entidad	3. Posible	2.Menor	5	Alto	Sí	Contratista	Etapa de ejecución si ocurre la situación	Pagos	Cumplimiento de las clausulas económicas y plan financiero	Revisión periódica o por facturación

RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:

Los riesgos de seguridad y privacidad de la información que se pueden presentar durante el desarrollo del Contrato son pérdida de la confidencialidad, integridad, disponibilidad y privacidad de los datos, los cuales podrían ocasionar que se interrumpa la prestación de los servicios.

	Nombre del Riesgo	Descripción del Riesgo	Clase d riesgo	Causas	Efectos	Probabilidad	Impacto	Controles
	Posibilidad de afectación reputacional, por la pérdida de disponibilidad de los servicios TICs, debido a la falta de seguimiento y monitoreo de las herramientas TICS- SGSI	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 TICs	Alta	Mayor	Aplicar el procedimiento de control de cambios
				Errores humanos	Violación a las seguridad			Implementar actualizaciones de las diferentes aplicaciones utilizadas en la Entidad
				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				
	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	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	Deficiencias en cultura de la seguridad de la información e Informática	Retrasos en los pr funcionarios y cont	Media	Mayor	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

	accesos no autorizados - SGSI			Vandalismo Informático	Sanciones legales y disciplinarias			Realizar la verificación de vulnerabilidades de la plataforma TICs
				Desconocimiento del manual de políticas de seguridad.	Afectación de la Entidad			Mantener operativas las herramientas tecnológicas
				Usuarios inconformes que puedan atentar contra la seguridad de la información				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 backup, 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				
	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 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			
	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	La información activa o cuando ha dejado de utilizarse debe gestionarse de una forma segura, porque la información clasificada o reservada, así como aquella	SGSI	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.
				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.

	carácter personal (datos personales), debido a la falta de controles para la protección de la información -SGSI	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.		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			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 Entidad			
				Desconocimiento procedimiento de eliminación de Documentos				
	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,	SGSI	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

		comprometiendo la Confidencialidad, Integridad y Disponibilidad de la información.			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

ALEJANDRO MESA MUÑOZ

COORDINADOR, GRUPO DE SOPORTE DE TI Y MESA DE AYUDA

Elaboró: Alejandro Mesa Muñoz, Coordinador del Grupo de Soporte de TI y Mesa de Ayuda

Revisó: Claudio Raul Ibarra Rodriguez, Abogado, Oficina de Tecnologías y Sistemas de Información