Plan de Seguridad y Privacidad de la Información

Dirección de Tecnología

2024

IU Digital de Antioquia

INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA

Historial de cambios

Versión	Fecha	Descripción del Cambio
01	30/01/2023	No aplica para la primera versión
02	26/01/2024	Se adecuaron las metas e indicadores al Plan de Desarrollo 2022-2026. Se actualizaron todos los componentes del plan.

Contenido

1. Introducción

La Institución Universitaria Digital de Antioquia se acoge a la estrategia de Gobierno Digital implementada en el país, y plasma en este plan los lineamientos y directrices a seguir para adaptarse a los requerimientos de los ciudadanos y la responsabilidad frente al manejo adecuado y confidencial de la información, por esta razón, propone el siguiente Plan de Seguridad y Privacidad de la Información para la vigencia 2024.

Siendo consciente de que la ciberseguridad y, en general, la seguridad de la información son componentes críticos y fundamentales dentro de la estrategia institucional, la IU Digital de Antioquia presenta el plan de seguridad y privacidad de la información, donde reconoce su importancia para el sector de la Educación Superior y ha identificado la información como el activo más importante y crítico para el desarrollo de sus funciones.

Este plan se elaboró teniendo en cuenta los lineamientos establecidos por el Gobierno nacional a través del Manual de Política de Gobierno Digital y del Modelo de Privacidad y Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones con el fin de crear requisitos de uso transparentes en el entorno híbrido de la información, mediante una óptica basada en la identificación y control de activos, gestión de riesgos y mitigación de posibles afectaciones en los recursos digitales que afecten la gestión y la continuidad del servicio.

Este plan se define teniendo en cuenta el contexto, las necesidades de la organización, las buenas prácticas y la normativa vigente establecida en la Norma Técnica Colombiana (NTC) ISO 27001 en todas sus versiones, Marco de Referencia de Arquitectura v. 2.0 propuesto por el ministerio de las TIC y lo establecido en los Decreto 1008 de 14 de junio 2018, 1078 de 2015, la Resolución 1519 de 2022, la Resolución 500 de 2021.

2. Objetivos

2.1. Objetivo general

Definir las acciones necesarias para incrementar la madurez en seguridad y privacidad de la Información en la Institución Universitaria Digital de Antioquia, de acuerdo con las estrategias de Gobierno Digital, MIPG, requerimientos de la entidad, disposiciones legales y buenas prácticas

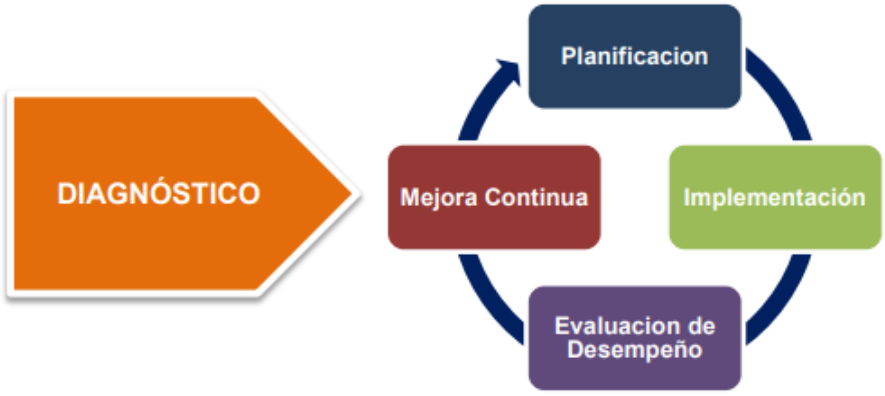
vigentes, tendientes a garantizar la integridad, confidencialidad, disponibilidad y privacidad de la información institucional.

2.2. Objetivos específicos

- Fortalecer y optimizar la gestión de seguridad y privacidad de la información al interior de la IU Digital de Antioquia, apoyando el cumplimiento de los objetivos estratégicos de la Institución.
- Fortalecer la cultura, el conocimiento y las habilidades de los colaboradores en los temas de seguridad y privacidad de la información en la IU Digital de Antioquia.
- Desarrollar estrategias que permitan la continuidad de los servicios tecnológicos prestados por la IU Digital de Antioquia, frente a situaciones adversas que impidan el normal funcionamiento y prestación de estos.
- Atender los requerimientos de seguridad de la información, seguridad digital y ciberseguridad establecidos por las diferentes entidades a nivel nacional y requisitos legales.
- Gestionar los riesgos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación tecnológica que puedan afectar la integridad, confidencialidad, disponibilidad y privacidad de la información.
- Identificar, clasificar y mantener actualizados los activos de información de la IU Digital de Antioquia.

3. Descripción del ciclo de operación

En el presente capítulo se explica el ciclo de funcionamiento del modelo de operación, a través de la descripción detallada de cada una de las cinco (5) fases que lo comprenden. Estas contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de las entidades.

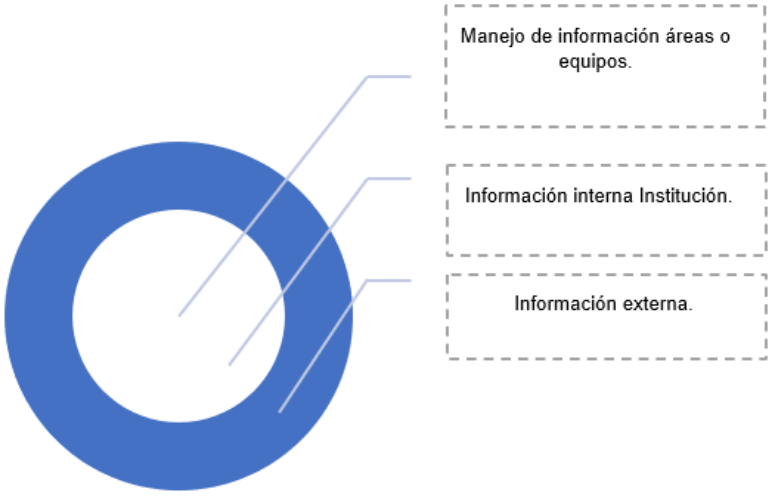


Gráfica 1. Fases del Plan de Seguridad y Privacidad de la Información

Estas fases suponen una correlación transversal de los procesos de evaluación y monitoreo en cada fase, teniendo como referencia un protocolo con tiempos establecidos para cada una de ellas. A continuación, se detalla cada fase y se especifican los instrumentos para el seguimiento.

3.1. Fase 1: Diagnóstico

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.



Gráfica 2. Momentos del diagnóstico

A continuación, se describe la matriz de evaluación de oportunidad para cada sector institucional.

FASE DE DIAGNÓSTICO EQUIPOS DE TRABAJO		
Indicador	**Meta**	**Guía**
Nivel de madurez del equipo de trabajo	Documento con estado de madurez	LI.ES.01 LI.ES.02 LI.GO.01 LI.GO.04 LI.GO.05 LI.GO.07 LI.ST.14

FASE DE DIAGNÓSTICO INSTITUCIONAL		
Indicador	**Meta**	**Guía**
Nivel de madurez de seguridad y privacidad de la información institucional.	Documento con estado de madurez en seguridad digital de la institucional	LI.ES.01 LI.ES.02 LI.GO.01 LI.GO.04 LI.GO.05 LI.GO.07 LI.ST.14

Indicador	**Meta**	**Guía**
Nivel de madurez de seguridad y privacidad de la información externa a la Institución	Documento con estado de madurez externo	LI.ES.01 LI.ES.02 LI.GO.01 LI.GO.04 LI.GO.05 LI.GO.07 LI.ST.14

IPv4 es la versión 4 del protocolo IP (Internet Protocol).
IPv6 es la versión 6 del Protocolo de Internet (IP por sus siglas en inglés, Internet Protocol)

3.2. Fase 2: Planificación

Partiendo de las metas de la fase de diagnóstico, se deben realizar encuentros periódicos para socializar y divulgar los hallazgos y los indicadores a cumplir en cada guía aplicada.

FASE DE PLANEACIÓN		
Indicador	**Meta**	**Guía**
Cumplimiento del Plan de Seguridad y Privacidad de la Información	Porcentaje de cumplimiento del Plan de Seguridad y Privacidad de la Información	LI.ES.09 LI.ES.10 LI.GO.01 LI.GO.04 LI.GO.07 LI.GO.08 LI.GO.09 LI.GO.10 LI.INF.01 LI.INF.02 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.SIS.22 LI.SIS.23 LI.SIS.01 LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12 LI.ST.13 LI.ST.14 LI.UA.01 LI.UA.02 LI.UA.03 LI.UA.04 LI.UA.05 LI.UA.06

3.3. Fase 3: Implementación

En esta fase se lleva a cabo la aplicación de todo lo desarrollado en la fase de diagnóstico y planificación, se tienen presente todas las guías aplicadas y los documentos generados como resultados del análisis y el trabajo colectivo.

FASE DE IMPLEMENTACIÓN		
Indicador	**Meta**	**Guía**
Porcentaje de implementación de las medidas de seguridad y privacidad de la información	90% de implementación de las medidas de seguridad y privacidad de la información	LI.GO.04 LI.GO.09 LI.GO.10 LI.GO.14 LI.GO.15 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.INF.15 LI.SIS.22 LI.SIS.23 LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.1 LI.UA.01 LI.UA.02 LI.UA.03 LI.UA.04 LI.UA.05 LI.UA.06

3.4. Fase 4: Evaluación del desempeño

La fase de evaluación del desempeño tiene como propósito principal hacer una evaluación y monitoreo a cada indicador y los resultados que este arroje, partiendo de los principios de efectividad, eficiencia y eficacia en cada uno de los procesos institucionales.

FASE EVALUACIÓN DEL DESEMPEÑO		
Indicador	**Meta**	**Guía**
Efectividad de la evaluación del desempeño del Plan de Seguridad y Privacidad de la Información	Porcentaje de cumplimiento de los objetivos de evaluación del desempeño del Plan de Seguridad y Privacidad de la Información	LI.ES.13 LI.GO.03 LI.GO.11 LI.GO.12 LI.INF.09 LI.INF.11 LI.INF.13 LI.INF.14 LI.INF.15 LI.SIS.23 LI.ST.05 LI.ST.06 LI.ST.08 LI.ST.15 LI.UA.07 LI.UA.08

3.5. Fase 5: Mejora continua

Consolidaremos los resultados obtenidos de la fase de evaluación de desempeño para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

FASE DE MEJORA CONTINUA		
Indicador	**Meta**	**Guía**
Nivel de reducción de los riesgos de seguridad y privacidad de la información	Reducción del 50% de los riesgos de seguridad y privacidad de la información	LI.ES.09 LI.ES.10 LI.GO.04 LI.GO.09 LI.GO.10 LI.GO.14 LI.GO.15 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.INF.15 LI.SIS.22 LI.SIS.23 LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12

4. Mapa de ruta y seguimiento

La implementación del Plan de Seguridad y Privacidad de la Información tiene lugar a partir del desarrollo de actividades y la ejecución de esfuerzos encaminados a su consecución, comprendiendo indicadores que facilitan la medición de las acciones e identificando plenamente la descripción de los productos y/o resultados alcanzados y esperados, de la siguiente manera:

N°	ACTIVIDAD	Meta establecida	Unidad de medida	Producto o servicio esperado
1. ACTIVOS DE INFORMACIÓN				
1.1	Actualización de los Instrumentos de gestión de la información.	2	Unidad	Actualización de la matriz de activos
1.2	Definir lineamientos para la gestión y uso de los activos	1	Unidad	Documento con procedimientos y guías para la gestión y uso de los activos.
2. RIESGOS				
2.1	Actualización de la matriz de riesgos de seguridad y privacidad de la información.	2	Unidad	Matriz de riesgos actualizada
3. SENSIBILIZACIÓN				
3.1	Definición del Plan de sensibilización	1	Unidad	Documento plan de sensibilización
4. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
4.1	Implementación de controles de seguridad	100	Porcentaje (Número de vulnerabilidades controladas / Número de vulnerabilidades identificadas con criticidad alta)	Documentación o reportes de las vulnerabilidades identificadas y controladas.
4.2	Revisión de los controles de seguridad establecidos.	2	Unidad	Herramienta de medición y diagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), semestral
4.3	Identificar acciones de mejora para fortalecer los controles de seguridad.	4	Unidad	Documento con acciones de mejora identificadas y sus controles.
4.4	Atención oportuna de incidentes y eventos informáticos.	100	Porcentaje (Número de incidentes y eventos informáticos atendidos / Número de incidentes y	Registro y documentación de las acciones sobre la gestión de los incidentes y/o eventos de seguridad presentados

			eventos informáticos reportados)	
5. PROTECCIÓN DE DATOS PERSONALES				
5.1	Seguimiento al Manual de Protección de Datos Personales	1	Unidad	Informe de Seguimiento y Recomendaciones
6. CONTINUIDAD DEL SERVICIO				
6.1	Diseñar el plan para la continuidad del servicio	1	Unidad	Plan para la continuidad del servicio de TI en la IU Digital
7. SEGURIDAD INFORMÁTICA				
7.1	Establecer análisis de vulnerabilidades en los sistemas y plataformas tecnológicas.	3	Unidad	Informe con análisis de vulnerabilidades

En ese sentido, el Plan de Seguridad y Privacidad de la Información será objeto de **un (1) seguimiento semestral**, conforme a los formatos dispuestos para tal fin en el Modelo de Operación por Procesos institucional.

5. Guías de referencia Ministerio de TIC

REFERENCIA	LINEAMIENTO	DESCRIPCIÓN
LI.ES.01	Entendimiento estratégico - LI.ES.01	Las instituciones de la administración pública deben contar con una estrategia de TI que esté alineada con las estrategias sectoriales, el Plan Nacional de Desarrollo, los planes sectoriales, los planes decenales, cuando existan, y los planes estratégicos institucionales. La estrategia de TI debe estar orientada a generar valor y a contribuir al logro de los objetivos estratégicos.
LI.ES.02	Definición de la Arquitectura Empresarial - LI.ES.02	Cada sector e institución, mediante un trabajo articulado, debe contar con una Arquitectura Empresarial que permita materializar su visión estratégica utilizando la tecnología como agente de transformación. Para ello, debe aplicar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI del país, teniendo en cuenta las características específicas del sector o la institución.

LI.ES.06	Políticas y estándares para la gestión y gobernabilidad de TI - LI.ES.06	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar y definir las políticas y estándares que faciliten la gestión y la gobernabilidad de TI, contemplando por lo menos los siguientes temas: seguridad, continuidad del negocio, gestión de información, adquisición, desarrollo e implantación de sistemas de información, acceso a la tecnología y uso de las facilidades por parte de los usuarios. Así mismo, se debe contar con un proceso integrado entre las instituciones del sector que permita asegurar el cumplimiento y actualización de las políticas y estándares de TI.
LI.ES.07	Plan de comunicación de la estrategia de TI - LI.ES.07	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir el plan de comunicación de la estrategia, las políticas, los proyectos, los resultados y los servicios de TI.
LI.ES.08	Participación en proyectos con componentes de TI - LI.ES.08	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe participar de forma activa en la concepción, planeación y desarrollo de los proyectos de la Institución que incorporen componentes de TI. Así mismo, debe asegurar la conformidad del proyecto con los lineamientos de la Arquitectura Empresarial definidos para la institución.
LI.ES.09	Control de los recursos financieros - LI.ES.09	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar de manera periódica el seguimiento y control de la ejecución del presupuesto y el plan de compras asociado a los proyectos estratégicos del PETI.
LI.ES.10	Gestión de proyectos de inversión - LI.ES.10	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe ser la responsable de formular, administrar, ejecutar y hacer seguimiento de las fichas de los proyectos de inversión requeridos para llevar a cabo la implementación de la Estrategia TI. El proceso de gestión de proyectos de inversión debe cumplir con los lineamientos que para este efecto establezca el Departamento Nacional de Planeación (DNP).
LI.ES.12	Evaluación de la gestión de la estrategia de TI - LI.ES.12	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar de manera periódica la evaluación de la gestión de la Estrategia TI, para determinar el nivel de avance y cumplimiento de las metas definidas en el PETI.
LI.ES.13	Tablero de indicadores - LI.ES.13	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un tablero de indicadores sectorial y por institución, que permita tener una visión integral de los avances y resultados en el desarrollo de la Estrategia TI.
LI.GO.01	Alineación del gobierno de TI - LI.GO.01	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar un esquema de Gobierno TI que estructure y direccione el flujo de las decisiones de TI, que garantice la integración y la alineación con la

		normatividad vigente, las políticas, los procesos y los servicios del Modelo Integrado de Planeación y Gestión de la institución.
LI.GO.03	Conformidad - LI.GO.03	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir y realizar actividades que conduzcan a evaluar, monitorear y direccionar los resultados de las soluciones de TI para apoyar los procesos internos de la institución. Debe, además, tener un plan específico de atención a aquellos procesos que se encuentren dentro de la lista de no conformidad del marco de las auditorías de control interno y externo de gestión, a fin de cumplir con el compromiso de mejoramiento continuo de la administración pública de la institución.
LI.GO.04	Cadena de Valor de TI - LI.GO.04	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el macroproceso de gestión de TI, según los lineamientos del Modelo Integrado de Planeación y Gestión de la institución, teniendo en cuenta el Modelo de gestión estratégica de TI.
LI.GO.05	Capacidades y recursos de TI - LI.GO.05	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir, direccionar, evaluar y monitorear las capacidades disponibles y las requeridas de TI, las cuales incluyen los recursos y el talento humano necesarios para ofrecer los servicios de TI.
LI.GO.07	Criterios de adopción y de compra de TI - LI.GO.07	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir los criterios y métodos que direccionen la toma de decisiones de inversión en Tecnologías de la Información (TI), buscando el beneficio económico y de servicio de la Institución. Para todos los proyectos en los que se involucren TI, se deberá realizar un análisis del costo total de propiedad de la inversión, en el que se incorporen los costos de los bienes y servicios, los costos de operación, el mantenimiento, el licenciamiento, el soporte y otros costos para la puesta en funcionamiento de los bienes y servicios por adquirir. Este estudio debe realizarse para establecer los requerimientos de financiación del proyecto. Debe contemplar los costos de capital (CAPEX) y los costos de operación (OPEX).
LI.GO.08	Retorno de la inversión de TI - LI.GO.08	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe establecer la relación costo-beneficio y justificar la inversión de los proyectos de TI. Para establecer el retorno de la inversión, se deberá estructurar un caso de negocio para el proyecto, con el fin de asegurar que los recursos públicos se utilicen para contribuir al logro de beneficios e impactos concretos de la institución. Debido a la imposibilidad de obtener retorno monetario en algunos casos, ya que se trata de gestiones sin ánimo de lucro, los beneficios deben contemplar resultados

		de mejoramiento del servicio, de la oportunidad, de la satisfacción del ciudadano y del bienestar de la población, entre otros.
LI.GO.09	Liderazgo de proyectos de TI - LI.GO.09	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe liderar la planeación, ejecución y seguimiento a los proyectos de TI. En aquellos casos en que los proyectos estratégicos de la Institución incluyan componentes de TI y sean liderados por otras áreas. La Dirección de Tecnologías y Sistemas de la Información, o quien haga sus veces, deberá liderar el trabajo sobre el componente de TI conforme con los lineamientos de la Arquitectura Empresarial de la Institución.
LI.GO.10	Gestión de proyectos de TI - LI.GO.10	El gerente de un proyecto, por parte de la Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, deberá evaluar, direccionar y monitorear lo relacionado con TI, incluyendo como mínimo los siguientes aspectos: alcance, costos, tiempo, equipo humano, compras, calidad, comunicación, interesados, riesgos e integración. Desde la estructuración de los proyectos de TI, y hasta el cierre de los mismos, se deben incorporar las acciones necesarias para gestionar los cambios que surjan.
LI.GO.11	Indicadores de gestión de los proyectos de TI - LI.GO.11	El gerente de un proyecto, por parte de la Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe monitorear y hacer seguimiento a la ejecución del proyecto, por medio de un conjunto de indicadores de alcance, tiempo, costo y calidad que permitan medir la eficiencia y efectividad del mismo.
LI.GO.12	Evaluación del desempeño de la gestión de TI - LI.GO.12	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar el monitoreo y evaluación de desempeño de la gestión de TI a partir de las mediciones de los indicadores del macroproceso de Gestión TI.
LI.GO.13	Mejoramiento de los procesos - LI.GO.13	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar áreas con oportunidad de mejora, de acuerdo con los criterios de calidad establecidos en el Modelo Integrado de Planeación y Gestión de la Institución, de modo que pueda focalizar esfuerzos en el mejoramiento de los procesos de TI para contribuir con el cumplimiento de las metas institucionales y del sector.
LI.GO.14	Gestión de proveedores de TI - LI.GO.14	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe administrar todos los proveedores y contratos para el desarrollo de los proyectos de TI. Durante el proceso contractual se debe aplicar un esquema de dirección, supervisión, seguimiento, control y recibo a satisfacción de los bienes y servicios contratados.

LI.GO.15	Transferencia de información y conocimiento - LI.GO.15	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe gestionar la transferencia de conocimiento asociado a los bienes y servicios contratados por la institución. Además, debe contar con planes de formación y de transferencia de conocimiento en caso de cambios del recurso humano interno.
LI.INF.01	Responsabilidad y gestión de Componentes de información - LI.INF.01	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir las directrices y liderar la gestión de los Componentes de información durante su ciclo de vida. Así mismo, debe trabajar en conjunto con las dependencias para establecer acuerdos que garanticen la calidad de la información.
LI.INF.02	Plan de calidad de los componentes de información - LI.INF.02	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un plan de calidad de los componentes de información que incluya etapas de aseguramiento, control e inspección, medición de indicadores de calidad, actividades preventivas, correctivas y de mejoramiento continuo de la calidad de los componentes.
LI.INF.09	Canales de acceso a los Componentes de información - LI.INF.09	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe garantizar los mecanismos que permitan el acceso a los servicios de información por parte de los diferentes grupos de interés, contemplando características de accesibilidad, seguridad y usabilidad.
LI.INF.10	Mecanismos para el uso de los Componentes de información - LI.INF.10	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe impulsar el uso de su información a través de mecanismos sencillos, confiables y seguros, para el entendimiento, análisis y aprovechamiento de la información por parte de los grupos de interés.
LI.INF.11	Acuerdos de intercambio de Información - LI.INF.11	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe establecer los Acuerdos de Nivel de Servicio (ANS) con las dependencias o instituciones para el intercambio de la información de calidad, que contemplen las características de oportunidad, disponibilidad y seguridad que requieran los Componentes de información.
LI.INF.13	Hallazgos en el acceso a los Componentes de información - LI.INF.13	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe generar mecanismos que permitan a los consumidores de los componentes de información reportar los hallazgos encontrados durante el uso de los servicios de información.
LI.INF.14	Protección y privacidad de Componentes de información - LI.INF.14	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe incorporar, en los atributos de los componentes de información, la información asociada con los responsables y políticas de la protección y privacidad de la información, conforme con la normativa de protección de datos

		de tipo personal y de acceso a la información pública.
LI.INF.15	Auditoría y trazabilidad de componentes de información - LI.INF.15	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información. Estos mecanismos deben ser considerados en el proceso de gestión de dichos componentes. Los sistemas de información deben implementar los criterios de trazabilidad y auditoría definidos para los Componentes de información que maneja.
LI.SIS.01	Definición estratégica de los sistemas de información - LI.SIS.01	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir la arquitectura de los sistemas de información teniendo en cuenta las relaciones entre ellos y la articulación con los otros dominios del Marco de Referencia.
LI.SIS.11	Ambientes independientes en el ciclo de vida de los sistemas de información - LI.SIS.11	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe disponer de ambientes independientes y controlados destinados para desarrollo, pruebas, operación, certificación y capacitación de los sistemas de información, y debe aplicar mecanismos de control de cambios de acuerdo con las mejores prácticas.
LI.SIS.22	Seguridad y privacidad de los sistemas de información - LI.SIS.22	En el diseño de sus sistemas de información, la Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe incorporar aquellos componentes de seguridad para el tratamiento de la privacidad de la información, la implementación de controles de acceso, así como los mecanismos de integridad y cifrado de la información.
LI.SIS.23	Auditoría y trazabilidad de los sistemas de información - LI.SIS.23	En el diseño de sus sistemas de información, la Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios.
LI.ST.05	Continuidad y disponibilidad de los servicios tecnológicos - LI.ST.05	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe garantizar que sus Servicios Tecnológicos estén respaldados con sistemas de alimentación eléctrica, mecanismos de refrigeración, soluciones de detección de incendios, sistemas de control de acceso y sistemas de monitoreo de componentes físicos que aseguren la continuidad y disponibilidad del servicio, así como la capacidad de atención y resolución de incidentes.

LI.ST.06	Alta disponibilidad de los servicios tecnológicos - LI.ST.06	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar capacidades de alta disponibilidad que incluyan balanceo de carga y redundancia para los servicios tecnológicos que afecten la continuidad del servicio de la institución, las cuales deben ser puestas a prueba periódicamente.
LI.ST.08	Acuerdos de Nivel de Servicios - LI.ST.08	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe velar por el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) para los Servicios Tecnológicos.
LI.ST.10	Planes de mantenimiento o - LI.ST.10	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar un plan de mantenimiento preventivo sobre toda la infraestructura y los servicios tecnológicos.
LI.ST.12	Gestión preventiva de los servicios tecnológicos - LI.ST.12	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe asegurarse de que la infraestructura que soporta los servicios tecnológicos de la Institución cuente con mecanismos de monitoreo para generar alertas tempranas ligadas a los umbrales de operación que tenga definidos.
LI.ST.13	Respaldo y recuperación de los servicios tecnológicos - LI.ST.13	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un proceso periódico de respaldo de la configuración de sus servicios tecnológicos, así como de la información almacenada en la infraestructura tecnológica. Este proceso debe ser probado periódicamente y debe permitir la recuperación íntegra de los servicios tecnológicos.
LI.ST.14	Análisis de vulnerabilidades - LI.ST.14	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el análisis de vulnerabilidades de la infraestructura tecnológica, a través de un plan de pruebas que permita identificar y tratar los riesgos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de un servicio de TI.
LI.ST.15	Monitoreo de seguridad de infraestructura tecnológica - LI.ST.15	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar controles de seguridad para gestionar los riesgos asociados al acceso, trazabilidad, modificación o pérdida de información que atenten contra la disponibilidad, integridad y confidencialidad de la información.
LI.ST.16	Tecnología verde - LI.ST.16	La Institución debe implementar un programa de correcta disposición final de los residuos tecnológicos, incluyendo las opciones de reutilización a través de otros programas institucionales con los que cuente el Gobierno nacional.
LI.UA.01	Estrategia de uso y apropiación - LI.UA.01	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de definir la estrategia de uso y apropiación de TI, articulada con la cultura organizacional de la institución, y de asegurar que su desarrollo contribuya con el

		logro de los resultados en la implementación de los proyectos de TI.
LI.UA.02	Matriz de interesados - LI.UA.02	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con una matriz de caracterización que identifique, clasifique y priorice los grupos de interés involucrados e impactados por los proyectos de TI.
LI.UA.03	Involucramiento y compromiso - LI.UA.03	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de asegurar el involucramiento y compromiso para llamar a la acción de los grupos de interés, partiendo desde la alta dirección hacia al resto de los niveles organizacionales, de acuerdo con la matriz de caracterización.
LI.UA.04	Esquema de incentivos - LI.UA.04	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de identificar y establecer un esquema de incentivos que, alineado con la estrategia de uso y apropiación, movilice a los grupos de interés para adoptar favorablemente los proyectos de TI.
LI.UA.05	Plan de formación - LI.UA.05	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de asegurar que el plan de formación de la Institución incorpora adecuadamente el desarrollo de las competencias internas requeridas en TI.
LI.UA.06	Preparación para el cambio - LI.UA.06	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de elaborar un plan de gestión del cambio para facilitar el uso y apropiación de los proyectos de TI. Este plan debe incluir las prácticas, procedimientos, recursos y herramientas que sean necesarias para lograr el objetivo.
LI.UA.07	Evaluación del nivel de adopción de TI - LI.UA.07	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con indicadores de uso y apropiación para evaluar el nivel de adopción de la tecnología y la satisfacción en su uso, lo cual permitirá desarrollar acciones de mejora y transformación.
LI.UA.08	Gestión de impactos - LI.UA.08	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de administrar los efectos derivados de la implantación de los proyectos de TI.
LI.UA.10	Acciones de mejora - LI.UA.10	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe diseñar acciones de mejora y transformación a partir del monitoreo de la implementación de su estrategia de uso y apropiación y de la aplicación de mecanismos de retroalimentación.

Acción	Nombre	Fecha
Proyectó y Elaboró:	César Alexander Zapata Jiménez	19/01/2024
Revisó:	Juan Andrés Díaz Mazo	22/01/2024
Revisó y Aprobó:	Jhonatan Arroyave Jaramillo	23/01/2024
Los anteriores, declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales y, por lo tanto, bajo nuestra responsabilidad presentamos para firma.		

IU Digital de Antioquia

INSTITUCIÓN UNIVERSITARIA
DIGITAL DE ANTIOQUIA