Plan de Seguridad y Privacidad de la Información

Institución Universitaria Digital de Antioquia

Dirección de Tecnología

2025

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.
03	05-12-2024	Se actualizaron las metas e indicadores al Plan de Desarrollo 2022-2026. Se actualizaron todos los componentes del plan

Contenido

Historial de cambios **2**
1. Introducción **4**
2. Objetivos **5**
2.1. Objetivo general 5
2.2. Objetivos específicos 5
3. Ciclo Operacional mejorado para 2025 **6**
3.1. Fase 1: Sensibilización y capacitación 6
3.2. Fase 2: Diagnóstico 7
3.3. Fase 3: Planificación 8
3.4. Fase 4: Implementación 10
3.5. Fase 5: Evaluación del desempeño 11
3.6. Fase 6: Mejora continua 12
4. Mapa de ruta y seguimiento **13**
5. Guías de referencia Ministerio de TIC **17**
Fuentes **18**

1. Introducción

La Institución Universitaria Digital de Antioquia reafirma su compromiso con la estrategia de Gobierno Digital implementada en el país, adoptando lineamientos que fortalecen su responsabilidad frente al manejo adecuado, confidencial y seguro de la información. En este marco, presenta el Plan de Seguridad y Privacidad de la Información 2025, como una herramienta estratégica para garantizar la integridad, disponibilidad y confidencialidad de los datos institucionales y de sus ciudadanos digitales.

Conscientes de que la ciberseguridad y la gestión de la información son pilares fundamentales en la Educación Superior, la Institución ha identificado la información como su activo más valioso. Este plan busca proteger dichos activos, asegurando la continuidad de sus servicios mediante el cumplimiento de normativas nacionales e institucionales y la implementación de buenas prácticas en seguridad y privacidad.

El presente documento se fundamenta en los lineamientos del Manual de Política de Gobierno Digital, el Modelo de Privacidad y Seguridad de la Información (MSPI) del Ministerio TIC, y estándares internacionales como la Norma Técnica Colombiana (NTC) ISO 27001 en todas sus versiones. Asimismo, integra el Marco de Referencia de Arquitectura Empresarial v. 2.0 y se ajusta a las normativas nacionales vigentes, incluyendo los Decretos 1008 de 2018 y 1078 de 2015, las Resoluciones 1519 de 2022, 500 de 2021 y la Resolución 746 de 2022, que refuerza los lineamientos para la gestión de riesgos asociados a proveedores y el tratamiento de datos personales en entornos digitales.

Este marco normativo responde a la necesidad de proteger la información en un ecosistema híbrido, promoviendo la confidencialidad, integridad y disponibilidad de los datos en todos los niveles, y estableciendo controles específicos para mitigar riesgos en el entorno digital.

Este plan adopta un enfoque basado en la identificación y gestión de riesgos, el control de activos y la mitigación de posibles afectaciones a los recursos digitales, promoviendo un entorno confiable que garantiza la continuidad de las operaciones institucionales en un ecosistema híbrido y dinámico.

2. Objetivos

2.1. Objetivo general

Definir e implementar acciones estratégicas y operativas que incrementen la madurez en seguridad y privacidad de la información en la Institución Universitaria Digital de Antioquia, en alineación con las estrategias de Gobierno Digital , el Modelo Integrado de Planeación y Gestión (MIPG) , las normativas nacionales vigentes, y las mejores prácticas internacionales, con el objetivo de garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional en un entorno de transformación digital.

2.2. Objetivos específicos

- Fortalecer el sistema de gestión de seguridad y privacidad de la información, integrando lineamientos nacionales actualizados como la Resolución 746 de 2022 y normas internacionales, para asegurar el cumplimiento de los objetivos estratégicos institucionales.
- Promover una cultura organizacional sólida en ciberseguridad, mediante la capacitación continua de los colaboradores en buenas prácticas, manejo seguro de la información y adopción de tecnologías emergentes.
- Diseñar e implementar estrategias para la continuidad del servicio tecnológico, asegurando la resiliencia frente a incidentes cibernéticos y otras situaciones adversas que puedan impactar la operación.
- Cumplir con los estándares legales y regulatorios nacionales, como los decretos y resoluciones vigentes, asegurando la gestión proactiva de la seguridad digital y la ciberseguridad.
- Gestionar de manera integral los riesgos asociados a la seguridad y privacidad de

la información, priorizando la protección de activos críticos y la mitigación de impactos en la operación tecnológica.

- Identificar, clasificar y mantener actualizados los activos de información institucional, asegurando su correcta gestión a lo largo de su ciclo de vida y su alineación con la arquitectura tecnológica de la institución.
- Incorporar tecnologías innovadoras para el monitoreo y control de la seguridad digital, fortaleciendo la capacidad de respuesta ante amenazas emergentes y la gestión eficiente de los recursos tecnológicos.

3. Ciclo Operacional mejorado para 2025

El ciclo operativo propuesto ha sido mejorado incorporando prácticas internacionales, adaptaciones para tecnologías emergentes y un enfoque integral que fortalece tanto los aspectos técnicos como culturales de la seguridad y privacidad de la información. Este modelo consta de seis fases, integrando una fase inicial de sensibilización para garantizar un entendimiento uniforme en toda la organización.

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: Sensibilización y capacitación

Objetivo: Crear una base cultural sólida para la seguridad y privacidad de la información en toda la organización.

Acciones:

1. **Capacitaciones iniciales:** Realizar talleres interactivos sobre la importancia de la seguridad y privacidad para el personal.
2. **Sensibilización organizacional:** Promover campañas internas con mensajes accesibles y alineados con los objetivos estratégicos.
3. **Evaluación de conocimientos:** Aplicar pruebas diagnósticas para medir el nivel inicial de comprensión.

INDICADOR	META	GUIA
Porcentaje de personal sensibilizado	80% del personal sensibilizado	**Ley 1581 de 2012 (Protección de Datos Personales)**: Proporciona directrices para la sensibilización en privacidad de datos personales.
Nivel de comprensión de seguridad de la información.	Asegurar que el 90% de los cursos de seguridad y privacidad de la información sean implementados y completados según el plan anual de capacitación.	**ISO 27001**: Sistema de gestión de seguridad de la información, específicamente el Control A.7.2.2 sobre concienciación y formación.

3.2. Fase 2: Diagnóstico

Objetivo: Determinar el estado actual de la organización en seguridad y privacidad de la información.

Acciones:

1. **Evaluación interna:** Determinar el nivel de madurez de los equipos de trabajo y la infraestructura tecnológica mediante la matriz de riesgos Institucional.
2. **Análisis externo:** Realizar un análisis estratégico profundo de las mejores prácticas con organizaciones similares y evaluar riesgos asociados a tendencias globales como ciberataques y tecnologías emergentes (p. ej., IA).
3. **Priorización:** Clasificar los hallazgos según su impacto y probabilidad, desarrollando un informe detallado.

INDICADOR	META	GUIA
Nivel de madurez en seguridad de la información	Alcanzar un nivel de madurez del 70% según la matriz de riesgos institucional	**ISO 21827 (SSE-CMM)**: Proporciona un marco para evaluar el nivel de madurez en la gestión de seguridad de la información dentro de una organización.
Cobertura del análisis comparativo con mejores prácticas.	Completar el análisis comparativo con al menos 5 organizaciones similares	**ISO 27001**: Estándar internacional para la gestión de la seguridad de la información, con principios de benchmarking y evaluación de mejores prácticas.

3.3. Fase 3: Planificación

Objetivo: Establecer estrategias y acciones prioritarias basadas en los resultados del diagnóstico.

Acciones:

1. **Definición de metas específicas:** Establecer objetivos medibles, como capacitación, infraestructura y políticas de seguridad.
2. **Desarrollo de planes detallados:** Crear planes específicos de mitigación, basados en los riesgos más críticos.
3. **Cronogramas optimizados:** Diseñar calendarios claros con hitos de cumplimiento para garantizar avances consistentes.

INDICADOR	META	GUIA
Cumplimiento de acciones del plan anual de seguridad y privacidad de la información.	Implementación del 90% de las acciones planificadas en el plan anual de seguridad y privacidad de la información.	**ISO 27001**: Esta norma internacional establece que las organizaciones deben tener un sistema de gestión de seguridad de la información (SGSI), que incluya el cumplimiento de metas específicas, como capacitación y políticas de seguridad.
Implementación de planes de mitigación de riesgos.	Completar el 80% de las medidas de mitigación para los riesgos críticos	**ISO 31000**: Estándar internacional sobre gestión del riesgo que proporciona directrices sobre la identificación, evaluación, mitigación y monitoreo de riesgos. Esta norma es clave para diseñar planes de mitigación de efectivos.

3.4. Fase 4: Implementación

Objetivo: Ejecutar las acciones planificadas asegurando el cumplimiento de los estándares establecidos.

Acciones:

1. **Automatización de procesos:** Mantener la continuidad del servicio de los sistemas de monitoreo y herramientas como tableros dinámicos.
2. **Despliegue de controles técnicos:** Aplicar medidas concretas como actualizaciones de sistemas, configuración de firewalls y controles de acceso basados en roles.
3. **Validación continua:** Realizar pruebas funcionales y de penetración para verificar la efectividad de las acciones implementadas.

INDICADOR	META	GUIA
Automatización de procesos y monitoreo continuo	Continuidad en un 95% de las herramientas de monitoreo y automatización de procesos en los sistemas críticos	**ISO 27001**: Establece que las organizaciones deben implementar controles automáticos para garantizar la seguridad de la información, incluidos los sistemas de monitoreo continuo.
Implementación de controles técnicos y pruebas de penetración.	Lograr el 95% de implementación de controles técnicos y realizar pruebas de penetración.	**OWASP** (Open Web Application Security Project): Ofrece guías detalladas sobre las pruebas de penetración y medidas específicas de seguridad, como firewalls y configuraciones de control de acceso.

3.5. Fase 5: Evaluación del desempeño

Objetivo: Monitorear y analizar el impacto de las acciones implementadas.

Acciones:

1. **Monitoreos:** Realizar revisiones trimestrales para obtener datos actualizados.
2. **Evaluación de efectividad:** Medir el cumplimiento de metas mediante indicadores clave como la reducción de incidentes.
3. **Feedback proactivo:** Implementar sesiones de retroalimentación con equipos y usuarios finales para ajustar estrategias en tiempo real.

INDICADOR	META	GUIA
Revisión de desempeño de controles de seguridad	Evaluar el 100% de los controles de seguridad implementados cada seis meses	**ISO 27001**: Asegura que se revisen periódicamente los controles de seguridad a través de evaluaciones de desempeño interno. Además, **NIST SP 800-53** recomienda realizar estas evaluaciones al menos de manera semestral para garantizar que los controles sean efectivos y estén alineados con las amenazas actuales.
Eficiencia en la gestión de incidentes de seguridad.	Actualizar sistemas de detección de riesgos informáticos con una cobertura del 95% de los sistemas críticos.	**NIST SP 800-53**: Establece que se debe medir la eficacia de los controles de seguridad, evaluando específicamente la reducción de incidentes y problemas de seguridad mediante el monitoreo continuo.

3.6. Fase 6: Mejora continua

Objetivo: Consolidar aprendizajes y diseñar acciones correctivas y preventivas.

Acciones:

1. **Revisión de resultados:** Integrar datos de desempeño para identificar áreas de mejora.
2. **Actualización de políticas:** Ajustar políticas internas considerando cambios normativos y tecnológicos.
3. **Innovación en estrategias:** Incorporar soluciones tecnológicas avanzadas, como machine learning, para predecir riesgos futuros.

INDICADOR	META	GUIA
Porcentaje de implementación de acciones correctivas basadas en la identificación de vulnerabilidades	Implementar al menos el 95% de las acciones correctivas pertinentes derivadas de las auditorías internas.	**ISO 9001** : Establece que las acciones correctivas deben implementarse eficientemente, siguiendo un ciclo de mejora continua y con evaluaciones periódicas para medir su efectividad.
Porcentaje de políticas revisadas tras evaluación interna	Realizar revisiones anuales para evaluar y ajustar el 95% de las recomendaciones relacionadas con seguridad y privacidad de la información, cuando sea pertinente.	**NIST SP 800-53** : Los controles de seguridad deben revisarse y ajustarse periódicamente, como parte del ciclo continuo de gestión de riesgos.

El ciclo operativo 2025 optimiza la estructura previa al incorporar una fase de sensibilización, mejorar el diagnóstico externo y priorizar tecnologías emergentes. Además, refuerza la importancia de la evaluación continua y la mejora ágil para mantener la seguridad y privacidad de la información como un eje transversal dentro de la organización. Este enfoque garantiza la sostenibilidad, el cumplimiento normativo y la adaptación a los retos tecnológicos futuros.

4. Mapa de ruta y seguimiento

Se presenta una versión actualizada del mapa de ruta y seguimiento para la implementación del Plan de Seguridad y Privacidad de la Información, basado en las fases y acciones que se han trabajado anteriormente. Este mapa refleja los esfuerzos para asegurar que todas las actividades estén alineadas con las mejores prácticas y los estándares requeridos, incorporando indicadores medibles para cada acción:

N°	ACTIVIDAD	META ESTABLECIDA	UNIDAD DE MEDIDA	PRODUCTO O SERVICIO ESPERADO
1	SENSIBILIZACIÓN Y CAPACITACIÓN			
1.1	Porcentaje de personal sensibilizado	80% del personal sensibilizado	1 Unidad	Registro de sesiones de sensibilización
1.2	Nivel de comprensión de seguridad de la información.	Asegurar que el 90% de los cursos de seguridad y privacidad de la información sean implementados y completados según el plan anual de capacitación.	1 Unidad	Informe de ejecución de capacitaciones (GESTIÓN HUMANA)

N°	ACTIVIDAD	META ESTABLECIDA	UNIDAD DE MEDIDA	PRODUCTO O SERVICIO ESPERADO
2	**DIAGNÓSTICO**			
2.1	Nivel de madurez en seguridad de la información	Alcanzar un nivel de madurez del 70% según la matriz de riesgos institucional	1 Unidad	Informe ejecutivo
2.2	Cobertura del análisis comparativo con mejores prácticas.	Completar el análisis comparativo con al menos 3 organizaciones similares	1 Unidad	Informe ejecutivo comparativo con otras Organizaciones
3	**PLANIFICACIÓN**			
3.1	Cumplimiento de acciones del plan anual de seguridad y privacidad de la información.	Implementación del 90% de las acciones planificadas en el plan anual de seguridad y privacidad de la información.	1 Unidad	Informe ejecutivo con el cumplimiento de las acciones planificadas en el plan anual de seguridad y privacidad de la información.
3.2	Implementación de planes de mitigación de riesgos.	Completar el 80% de las medidas de mitigación para los riesgos críticos	1 Unidad	Informe ejecutivo con la implementación de procesos de mitigación para los riesgos críticos
4	**IMPLEMENTACIÓN**			

N°	ACTIVIDAD	META ESTABLECIDA	UNIDAD DE MEDIDA	PRODUCTO O SERVICIO ESPERADO
4.1	Automatización de procesos y monitoreo continuo	Continuidad en un 95% de las herramientas de monitoreo y automatización de procesos en los sistemas críticos	1 Unidad	Informe ejecutivo con la disponibilidad del servicio de herramientas de monitoreo y automatización
4.2	Implementación de controles técnicos y pruebas de penetración.	Lograr el 95% de implementación de controles técnicos y realizar pruebas de penetración.	1 Unidad	Informe ejecutivo con implementación de controles técnicos y resultados de pruebas de penetración.
5	**EVALUACIÓN DEL DESEMPEÑO**			
5.1	Revisión de desempeño de controles de seguridad	Evaluar el 100% de los controles de seguridad implementados cada seis meses	1 Unidad	Informe ejecutivo con controles de seguridad implementados
5.2	Eficiencia en la gestión de incidentes de seguridad.	Actualizar sistemas de detección de riesgos informáticos con una cobertura del 95% de los sistemas críticos.	1 Unidad	Informe ejecutivo con la actualización de sistemas de detección de riesgos
6	**MEJORA CONTINUA**			

N°	ACTIVIDAD	META ESTABLECIDA	UNIDAD DE MEDIDA	PRODUCTO O SERVICIO ESPERADO
6.1	Porcentaje de implementación de acciones correctivas basadas en la identificación de vulnerabilidades	Implementar al menos el 95% de las acciones correctivas pertinentes derivadas de las auditorías internas.	1 Unidad	Informe ejecutivo con las acciones correctivas derivadas de las auditorías internas.
6.2	Porcentaje de políticas revisadas tras evaluación interna	Realizar revisiones anuales para evaluar y ajustar el 95% de las recomendaciones relacionadas con seguridad y privacidad de la información, cuando sea pertinente.	1 Unidad	Informe ejecutivo con ajustes de las recomendaciones en seguridad y privacidad de la información.

El Plan de Seguridad y Privacidad de la Información será objeto de un seguimiento semestral, realizado conforme a los formatos y procedimientos establecidos en el Modelo de Operación por Procesos Institucionales. Este seguimiento permitirá evaluar el cumplimiento de los estándares definidos y asegurar la mejora continua en la gestión de la seguridad y privacidad de la información, adaptándose a los avances tecnológicos y normativos, con el objetivo de garantizar la protección adecuada de los activos informáticos y de los datos personales en la organización.

5. Guías de referencia Ministerio de TIC

REFERENCIA	LINEAMIENTO	DESCRIPCIÓN
ISO/IEC 27001	Gestión de la seguridad de la información	Norma internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Ayuda a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de la información mediante un enfoque sistemático de gestión de riesgos. Se aplica globalmente y es uno de los marcos más reconocidos en cuanto a seguridad de la información.
Ley 1581 de 2012	Protección de datos personales	Ley colombiana que regula la protección de datos personales, estableciendo los lineamientos para el manejo y tratamiento de información personal en Colombia. Busca garantizar derechos como el acceso, corrección y eliminación de datos personales, y la transparencia en su manejo.
Norma NIST SP 800-53	Controles de seguridad y privacidad	Estándar del Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. UU. que proporciona un marco de controles de seguridad para proteger la infraestructura crítica de la información en las organizaciones. Su uso es ampliamente adoptado para la seguridad cibernética, y también se adapta a la legislación colombiana en materia de seguridad tecnológica.

Fuentes

1. **ISO / IEC 27001:2013** - Sistemas de gestión de la seguridad de la información (ISO.org)
2. **Ley 1581 de 2012:** "Ley Estatutaria 1581 de 2012" (Congreso de Colombia)
3. **NIST SP 800-53:** "Controles de seguridad y privacidad para sistemas de información y organizaciones" (NIST.gov)

Estos documentos están enfocados en normas internacionales y nacionales que guían las prácticas de seguridad de la información, protección de datos personales y control de riesgos.

Acción	Nombre	Fecha
Proyectó y Elaboró:	César Alexander Zapata Jiménez	20/01/2025
Revisó:	César Luis Vásquez Suárez Mónica Andrea Santa Escobar	22/01/2025
Revisó y Aprobó:	Jhonatan Arroyave Jaramillo	23/01/2025
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