Política de Seguridad Digital

Institución Universitaria Publica de Bello

INTRODUCCION

El Modelo Integrado de Planeación y Gestión (MIPG), adoptado en Colombia mediante el Decreto 1499 de 2017, constituye el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de la Institución Universitaria Pública, con el propósito de generar resultados que respondan al Plan de Desarrollo Institucional y a las necesidades de la comunidad académica y la ciudadanía, bajo principios de integridad, eficiencia y calidad en el servicio. Su implementación fortalece la capacidad institucional, promueve la mejora continua, consolida la cultura del control interno y aumenta la confianza en la gestión universitaria.

En este contexto, la Política de Seguridad Digital se articula con la Política Nacional de Seguridad Digital establecida en el Documento CONPES 3854 de 2016, la cual orienta a las entidades públicas en la identificación, gestión y mitigación de los riesgos asociados al entorno digital. Para la Universidad, esto implica proteger la información académica, administrativa y financiera, garantizar la continuidad de los servicios tecnológicos y salvaguardar los datos personales de estudiantes, docentes y funcionarios.

Dado que la tecnología es un recurso estratégico para el cumplimiento de la misión institucional, resulta indispensable establecer lineamientos claros de seguridad de la información que definan controles, responsabilidades y buenas prácticas, con el fin de prevenir la alteración, pérdida, fuga o indisponibilidad de la información, fortalecer la gestión del riesgo y asegurar la confiabilidad de los sistemas que soportan los procesos académicos y administrativos.

1.PRESENTACION

La Institución universitaria publica de bello reconoce la información como un activo estratégico fundamental para el cumplimiento de su misión institucional, por lo cual establece la presente Política de Seguridad Digital con el fin de:

La Institución Universitaria Pública de Bello, en su compromiso permanente con el fortalecimiento de la infraestructura tecnológica y la adecuada gestión de las Tecnologías de la Información y las Comunicaciones (TIC), establece lineamientos, directrices y estándares orientados a garantizar la protección de la información institucional mediante la implementación de la Política de Seguridad Digital, en concordancia con los principios de la estrategia de Gobierno Digital y las buenas prácticas en seguridad de la información.

La presente política tiene como propósito preservar la confidencialidad, integridad, disponibilidad y privacidad de los activos de información institucionales, promoviendo su uso responsable, seguro y eficiente, así como la protección de los datos personales de estudiantes, docentes, funcionarios, contratistas y demás partes interesadas, contribuyendo al cumplimiento de la misión institucional y al fortalecimiento de la confianza en los servicios digitales ofrecidos por la institución.

De igual manera, esta política se articula con los lineamientos establecidos en la Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital – Diseño de Controles en Entidades Públicas, emitida por el Departamento Administrativo de la Función Pública y la Secretaría de Transparencia de la Presidencia de la República, especialmente en los componentes relacionados con el análisis del contexto digital, la identificación de activos de información, la gestión de amenazas y vulnerabilidades, el tratamiento de riesgos de seguridad digital y los mecanismos de monitoreo y reporte.

La declaración de la Política de Seguridad Digital Institucional busca proteger de manera integral los activos de información, incluyendo los grupos de valor, procesos académicos y administrativos, servicios tecnológicos, sistemas de información, infraestructura tecnológica, hardware y software, mediante la definición de lineamientos y controles que permitan gestionar adecuadamente los riesgos de seguridad digital en todos los procesos institucionales.

Así mismo, la política se enmarca en el Modelo Integrado de Planeación y Gestión (MIPG) y el Modelo de Seguridad y Privacidad de la Información (MSPI), promoviendo una cultura organizacional basada en la gestión del riesgo, la mejora continua, el cumplimiento normativo y la responsabilidad en el manejo de la información.

La implementación de esta Política de Seguridad Digital permitirá a la Institución fortalecer sus capacidades para prevenir, detectar y responder ante incidentes de seguridad de la información, garantizando la continuidad de los servicios académicos y administrativos, la protección de los datos y el cumplimiento de los objetivos estratégicos institucionales.

- Proteger los activos de información.
- Garantizar la continuidad de los servicios tecnológicos.
- Reducir riesgos de ciberseguridad.
- Generar confianza en los usuarios y partes interesadas.
- Cumplir con los requisitos legales y normativos.

2.OBJETIVOS

2.1 Objetivo General

Establecer los lineamientos, estrategias y controles necesarios para la gestión de la seguridad digital en la Institución Universitaria Pública de Bello, con el fin de proteger los activos de información institucionales, garantizando la confidencialidad, integridad, disponibilidad y privacidad de la información, mediante la identificación, análisis, tratamiento y mitigación de los riesgos asociados al uso de las tecnologías de la información y las comunicaciones, en concordancia con la normatividad vigente y los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) y el Modelo de Seguridad y Privacidad de la Información (MSPI).

2.2 Objetivos Específicos

1. **Identificar, clasificar y proteger los activos de información institucional**, estableciendo responsables y controles que garanticen la confidencialidad, integridad y disponibilidad de la información.
2. **Implementar un proceso de gestión de riesgos de seguridad digital**, que permita prevenir, detectar y mitigar amenazas y vulnerabilidades que puedan afectar los sistemas de información y la infraestructura tecnológica institucional.
3. **Fortalecer la seguridad de la infraestructura tecnológica y los servicios digitales**, mediante la aplicación de controles técnicos, administrativos y físicos que aseguren la operación confiable de los sistemas institucionales.
4. **Garantizar la protección de los datos personales y la continuidad de los servicios tecnológicos**, mediante el cumplimiento de la normatividad vigente, la gestión de incidentes de seguridad y la implementación de copias de seguridad y planes de contingencia.

3. **ALCANCE**

La presente Política de Seguridad Digital aplica a todos los procesos, activos de información, recursos tecnológicos, sistemas de información y servicios digitales de la Institución Universitaria Pública de Bello, independientemente de su ubicación física o modalidad de acceso, con el propósito de garantizar la protección de la información institucional en términos de confidencialidad, integridad, disponibilidad y privacidad.

El alcance comprende a todos los funcionarios, docentes, estudiantes, contratistas, proveedores y terceros que tengan acceso o hagan uso de los activos de información y recursos tecnológicos institucionales, quienes deberán cumplir con los lineamientos establecidos en esta política.

Así mismo, incluye la infraestructura tecnológica institucional, tales como servidores, redes de comunicaciones, equipos de cómputo, dispositivos móviles, sistemas de almacenamiento, plataformas académicas y administrativas, servicios en la nube, aplicaciones institucionales, correo electrónico y demás servicios tecnológicos que soportan la operación de la institución.

La política aplica a toda la información generada, procesada, almacenada, transmitida o custodiada por la institución, sin importar su formato (digital o físico) o nivel de clasificación (pública, interna, confidencial o reservada), durante todas las etapas de su ciclo de vida, desde su creación o captura hasta su disposición final o eliminación.

Igualmente, el alcance cubre todas las sedes institucionales, entornos de trabajo remoto, accesos externos autorizados y cualquier escenario en el cual se utilicen recursos tecnológicos o se gestione información institucional.

Se exceptúan únicamente aquellos casos que por disposición legal expresa cuenten con regulaciones específicas, sin perjuicio de la aplicación de los principios generales de seguridad de la información establecidos en la presente política.

4. **RESPONSABLE**

La responsabilidad de la implementación, mantenimiento, seguimiento y mejora continua de la presente Política de Seguridad Digital estará a cargo del **Área de Tecnologías de la Información y las Comunicaciones (TIC)** de la Institución Universitaria Pública de Bello, o quien haga sus veces, en articulación con las dependencias institucionales y bajo la orientación del Comité Institucional de Gestión y Desempeño.

El líder o responsable del proceso de Tecnologías de la Información será el encargado de coordinar las acciones necesarias para garantizar la adecuada gestión de la seguridad digital, incluyendo la identificación de riesgos, la implementación de controles, la gestión de incidentes de seguridad, la protección de los activos de información y el cumplimiento de la normatividad vigente.

Así mismo, la Alta Dirección será responsable de aprobar la política, asignar los recursos necesarios para su implementación y promover el cumplimiento de los lineamientos establecidos, mientras que todos los funcionarios, docentes, estudiantes, contratistas y terceros que tengan acceso a los activos de información institucional deberán cumplir las disposiciones contenidas en la presente política y reportar oportunamente cualquier incidente o situación que pueda comprometer la seguridad de la información.

5. **MARCO JURÍDICO Y LEGAL**

La presente Política de Seguridad Digital se fundamenta en la Constitución Política de Colombia, la normatividad vigente en materia de tecnologías de la información, protección de datos personales, transparencia, gestión documental, seguridad y gobierno digitales, así como en estándares y lineamientos nacionales e internacionales aplicables a las entidades públicas.

A continuación, se relacionan las principales normas que soportan la adopción e implementación de la presente política:

Normativa Constitucional

- **Constitución Política de Colombia (1991)** Artículos 15, 20 y 74, relacionados con el derecho fundamental al habeas data, la protección de la información personal y el acceso a la información pública.

NORMATIVA	EPIGRAFE
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal y se crea el bien jurídico de la protección de la información y de los datos, estableciendo los delitos informáticos.
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones (TIC).
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1928 de 2018	Por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia de Budapest.
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7° de la ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Decreto 103 de 2015	Reglamenta parcialmente la Ley 1712 de 2014 sobre transparencia y acceso a la información.
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector Tecnologías de la Información y las Comunicaciones.
Decreto 612 de 2018	Establece directrices para la integración de planes institucionales y estratégicos al Plan de Acción.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital.

6. DEFINICIÓN DE LA POLÍTICA

La Institución Universitaria Pública de Bello se compromete a implementar, mantener y mejorar continuamente la seguridad digital, garantizando la protección de los activos de información institucionales mediante la adopción de controles técnicos, administrativos y organizacionales que permitan preservar la confidencialidad, integridad, disponibilidad y privacidad de la información, así como la protección de los datos personales de estudiantes, docentes, funcionarios, contratistas y demás partes interesadas.

La política establece lineamientos y directrices orientadas a la gestión de los riesgos de seguridad digital asociados al uso de las Tecnologías de la Información y las Comunicaciones (TIC), con el propósito de prevenir incidentes de seguridad, reducir vulnerabilidades, asegurar la continuidad de los servicios tecnológicos y fortalecer la confianza en los procesos académicos y administrativos de la institución.

Así mismo, la Institución asignará los recursos humanos, tecnológicos, administrativos y financieros necesarios para la adecuada implementación de esta política, garantizando el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables, en concordancia con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), el Modelo de Seguridad y Privacidad de la Información (MSPI) y las buenas prácticas nacionales e internacionales en seguridad de la información.

La implementación de la Política de Seguridad Digital se realizará mediante un enfoque basado en la gestión de riesgos, la mejora continua y la responsabilidad compartida de todos los miembros de la comunidad institucional, quienes deberán cumplir las disposiciones establecidas y reportar cualquier situación que pueda comprometer la seguridad de la información.

7. PLAN DE ACCIÓN PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL

El presente plan de acción tiene como propósito establecer las estrategias, actividades y responsables necesarios para la implementación, mantenimiento y mejora continua de la Política de Seguridad Digital, garantizando la protección de los activos de información institucionales y la gestión adecuada de los riesgos asociados al entorno digital.

Categoría	Estrategia	Actividades	Responsable	Periodicidad
Gobierno de Seguridad Digital	Implementar el MSPI	Diseñar, documentar y aprobar políticas, procedimientos y controles de seguridad digital	Área TIC	Anual
		Conformar o fortalecer el comité de seguridad digital	Alta Dirección / TIC	Anual
Gestión de Activos de Información	Inventario de activos	Identificar, clasificar y actualizar inventario de activos de información	Área TIC / Dependencias	Permanente
Gestión de Riesgos	Gestión de riesgos de seguridad digital	Identificar amenazas, vulnerabilidades y riesgos	Área TIC	Anual

		Elaborar y actualizar matriz de riesgos	Área TIC	Anual
Controles Tecnológicos	Fortalecimiento de infraestructura	Implementar antivirus, firewall, control de accesos y actualizaciones de seguridad	Área TIC	Permanente
		Implementar mecanismos de respaldo y recuperación de información	Área TIC	Permanente
Gestión de Incidentes	Procedimiento de incidentes	Diseñar e implementar procedimiento de gestión de incidentes de seguridad	Área TIC	Anual
		Establecer canales de reporte de incidentes	Área TIC	Permanente
Continuidad del Servicio	Plan de continuidad	Diseñar plan de continuidad y recuperación ante desastres	Área TIC	Anual
Capacitación y Cultura	Sensibilización	Realizar campañas de concientización en seguridad digital	Área TIC / Talento Humano	Semestral

		Capacitar funcionarios y usuarios en buenas prácticas	Área TIC	Semestral
Monitoreo y Seguimiento	Evaluación y mejora	Realizar auditorías internas y revisiones de seguridad	Área TIC / Control Interno	Anual
		Definir indicadores de seguridad digital	Área TIC	Anual

8. LINEAMIENTOS GENERALES DE LA POLÍTICA

La Institución Universitaria Pública de Bello establece los siguientes lineamientos generales para garantizar la adecuada gestión de la seguridad digital y la protección de los activos de información institucionales:

1. Protección de la Información Institucional

Todos los funcionarios, docentes, estudiantes, contratistas y terceros que tengan acceso a los activos de información institucional deberán velar por la seguridad de la información bajo los principios de confidencialidad, integridad, disponibilidad y privacidad, cumpliendo las disposiciones establecidas en la presente política y en la normatividad vigente.

2. Uso Adecuado de los Recursos Tecnológicos

Los recursos tecnológicos institucionales, incluyendo equipos de cómputo, redes, sistemas de información, correo electrónico, aplicaciones y acceso a internet, deberán utilizarse exclusivamente para el cumplimiento de las funciones académicas, administrativas o institucionales autorizadas, quedando prohibido su uso para actividades personales que puedan comprometer la seguridad de la información o la operación institucional.

3. Control de Acceso

Cada usuario deberá contar con credenciales de acceso únicas e intransferibles para el uso de los sistemas de información y servicios tecnológicos institucionales. El acceso a la información deberá otorgarse conforme a los perfiles y responsabilidades asignadas, aplicando el principio de mínimo privilegio.

4. Gestión de Activos de Información

Todos los activos de información deberán estar debidamente identificados, inventariados y contar con un responsable designado para su custodia y protección. Los propietarios de los activos deberán garantizar su uso adecuado y reportar cualquier incidente de seguridad que pueda afectarlos.

5. Seguridad de Equipos y Dispositivos

Los equipos tecnológicos institucionales deberán utilizarse exclusivamente para fines institucionales y contar con las medidas de seguridad definidas por el área de Tecnologías de la Información, incluyendo antivirus, actualizaciones de seguridad y controles de acceso. La salida de equipos fuera de las instalaciones institucionales deberá contar con autorización previa.

6. Instalación de Software

Se prohíbe la instalación de software no autorizado en los equipos institucionales. Toda instalación deberá ser realizada o aprobada por el área de Tecnologías de la Información, garantizando el cumplimiento de licencias y la seguridad del sistema.

7. Manejo de Información y Documentos

La información institucional, tanto en formato físico como digital, deberá ser gestionada conforme a los lineamientos de gestión documental y seguridad de la información, garantizando su protección durante todo el ciclo de vida, desde su creación hasta su eliminación o disposición final.

8. Uso del Correo Electrónico Institucional

El correo electrónico institucional deberá ser utilizado únicamente para fines institucionales. Los usuarios deberán adoptar buenas prácticas de seguridad, evitando abrir correos sospechosos, enlaces desconocidos o archivos adjuntos de origen no confiable.

9. Protección contra Amenazas Informáticas

Toda información proveniente de dispositivos externos o descargas de internet deberá ser analizada mediante herramientas de seguridad antes de su uso. Los usuarios deberán evitar el acceso a sitios web que representen riesgos de seguridad o afecten la productividad institucional.

10. Gestión de Incidentes de Seguridad

Los usuarios deberán reportar de manera inmediata cualquier incidente de seguridad digital, pérdida de información, accesos no autorizados o situaciones que puedan comprometer la seguridad de los activos de información, conforme a los procedimientos establecidos por la institución.

11. Copias de Seguridad y Continuidad del Servicio

La institución implementará mecanismos de respaldo de información y planes de contingencia que garanticen la disponibilidad y recuperación de los servicios tecnológicos ante fallas, incidentes o desastres.

12. Protección de Datos Personales

El tratamiento de datos personales se realizará conforme a la normativa vigente en materia de protección de datos personales, garantizando su confidencialidad, uso autorizado y protección contra accesos no autorizados.

13. Responsabilidad de los Usuarios

Cada usuario será responsable del uso adecuado de los recursos tecnológicos asignados y de la información bajo su custodia, así como del cumplimiento de las disposiciones establecidas en la presente política.

14. Cumplimiento Normativo

La institución garantizará el cumplimiento de la normatividad vigente en materia de seguridad digital, protección de datos personales, gestión documental y gobierno digital, promoviendo la mejora continua de los controles de seguridad.

15. Monitoreo y Seguimiento

La Institución podrá realizar actividades de monitoreo, auditoría y seguimiento sobre el uso de los recursos tecnológicos institucionales, con el fin de verificar el cumplimiento de la política y prevenir riesgos de seguridad digital.

9. **POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD**

La Institución Universitaria Pública de Bello reconoce la importancia de proteger la información personal e institucional, garantizando el adecuado tratamiento de los datos conforme a los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso restringido, seguridad y confidencialidad, en cumplimiento de la normatividad vigente.

1. Protección de Datos Personales

La institución garantizará la protección de los datos personales de estudiantes, docentes, funcionarios, contratistas, egresados y terceros, adoptando medidas técnicas, administrativas y organizativas que eviten la pérdida, alteración, acceso no autorizado o uso indebido de la información.

2. Tratamiento de la Información

El tratamiento de datos personales se realizará únicamente para fines institucionales legítimos, académicos, administrativos o legales, conforme a las autorizaciones otorgadas por los titulares de la información y las disposiciones normativas aplicables.

3. Confidencialidad de la Información

Toda persona que tenga acceso a información institucional deberá mantener la confidencialidad de esta, incluso después de finalizar su vínculo laboral, contractual o académico con la institución. La información clasificada como confidencial o reservada no podrá divulgarse sin autorización expresa.

4. Acceso a la Información

El acceso a la información estará restringido únicamente a las personas autorizadas, conforme a sus funciones y responsabilidades. Se aplicarán controles de acceso lógico y físico para proteger los datos contra accesos no autorizados.

5. Uso de la Información

La información institucional no podrá ser utilizada para fines personales, comerciales o diferentes a los establecidos por la institución. Se prohíbe la copia, reproducción, distribución o divulgación de información sin autorización previa.

6. Responsabilidad de los Usuarios

Los usuarios que accedan a información institucional serán responsables de su adecuada protección, uso correcto y custodia, evitando compartir credenciales de acceso o permitir el uso indebido de la información bajo su responsabilidad.

7. Transferencia y Compartición de Datos

La transferencia de información a terceros solo se realizará cuando exista autorización legal, contractual o consentimiento del titular, garantizando siempre las medidas de seguridad necesarias para su protección.

8. Conservación de la Información

Los datos personales e institucionales serán conservados únicamente durante el tiempo necesario para cumplir la finalidad para la cual fueron recolectados, conforme a las normas de gestión documental y requisitos legales vigentes.

9. Derechos de los Titulares

Los titulares de los datos personales podrán ejercer sus derechos de acceso, actualización, rectificación, supresión y revocatoria de autorización, conforme a los procedimientos establecidos por la institución y la legislación aplicable.

10. Incidentes de Privacidad

Cualquier incidente que comprometa la confidencialidad, integridad o disponibilidad de la información deberá ser reportado de manera inmediata al área de Tecnologías de la Información o a la dependencia responsable, para la activación de los protocolos de atención y mitigación correspondientes.

11. Compromiso Institucional

La institución promoverá la cultura de protección de datos personales y confidencialidad de la información mediante procesos de capacitación, sensibilización y mejora continua de los controles de seguridad.

10. **SEGURIDAD DE EQUIPOS Y COMPUTADORES**

La Institución Universitaria Pública de Bello establece lineamientos para garantizar la protección de los equipos informáticos, dispositivos tecnológicos y recursos de procesamiento de información, con el fin de prevenir accesos no autorizados,

pérdida de información, daños físicos o lógicos y riesgos asociados a la seguridad digital.

1. Uso Adecuado de los Equipos

Los equipos de cómputo institucionales deberán ser utilizados exclusivamente para el cumplimiento de las funciones académicas, administrativas y misionales de la institución. Se prohíbe el uso indebido para fines personales, actividades ilícitas o que comprometan la seguridad de la información institucional.

2. Control de Acceso

Todos los equipos deberán contar con mecanismos de autenticación mediante usuario y contraseña segura o métodos de autenticación definidos por la institución. Las credenciales de acceso son personales e intransferibles.

3. Protección contra Software Malicioso

Los equipos institucionales deberán contar con software antivirus, antimalware y mecanismos de protección actualizados, administrados por el área de Tecnologías de la Información, con el fin de prevenir infecciones y ataques informáticos.

4. Actualizaciones y Parches de Seguridad

Los sistemas operativos, aplicaciones y programas instalados deberán mantenerse actualizados con los últimos parches de seguridad disponibles, bajo la supervisión del área responsable de tecnología.

5. Instalación de Software

La instalación de software en los equipos institucionales solo podrá ser realizada o autorizada por el área de Tecnologías de la Información. Se prohíbe la instalación de programas sin licencia o no autorizados.

6. Protección Física de los Equipos

Los equipos deberán ubicarse en espacios seguros que reduzcan el riesgo de robo, daño o manipulación no autorizada. Cuando aplique, deberán implementarse mecanismos de seguridad física como guayas de seguridad, controles de acceso a oficinas o sistemas de vigilancia.

7. Dispositivos Portátiles

Los computadores portátiles, tabletas, dispositivos móviles y memorias USB institucionales deberán ser protegidos mediante contraseñas, cifrado de información cuando sea necesario y medidas que reduzcan el riesgo de pérdida o robo.

8. Copias de Seguridad

La información institucional almacenada en los equipos deberá contar con mecanismos de respaldo conforme a los lineamientos de copias de seguridad definidos por la institución, evitando la pérdida de información crítica.

9. Uso de Dispositivos Externos

El uso de dispositivos de almacenamiento externos deberá ser controlado y autorizado cuando sea necesario, con el fin de prevenir fugas de información o propagación de software malicioso.

10. Mantenimiento de Equipos

El mantenimiento preventivo y correctivo de los equipos será realizado por personal autorizado. Antes de realizar mantenimiento o disposición final de los equipos, deberá garantizarse la eliminación segura de la información almacenada.

11. Reporte de Incidentes

Los usuarios deberán reportar inmediatamente cualquier incidente de seguridad relacionado con equipos de cómputo, tales como pérdida, robo, daño, acceso no autorizado o sospecha de infección por software malicioso.

12. Responsabilidad de los Usuarios

Los funcionarios, docentes, estudiantes y contratistas que tengan asignados equipos institucionales serán responsables de su cuidado, uso adecuado y protección, conforme a las políticas institucionales vigentes.

11. SEGUIMIENTO Y MEDICIÓN DE LA POLÍTICA

La Institución Universitaria Pública de Bello realizará el seguimiento y la medición de la Política de Seguridad Digital con el propósito de evaluar su nivel de cumplimiento, efectividad, eficiencia y mejora continua, garantizando la adecuada

protección de los activos de información y el fortalecimiento de la gestión de riesgos de seguridad digital.

1. Mecanismos de Seguimiento

El seguimiento de la política se realizará mediante:

- Evaluaciones periódicas del cumplimiento de los lineamientos establecidos.
- Auditorías internas y externas de seguridad de la información.
- Revisión de controles de seguridad implementados.
- Monitoreo de incidentes de seguridad digital.
- Verificación del cumplimiento de requisitos legales y normativos.
- Evaluación de riesgos de seguridad de la información.

2. Indicadores de Medición

Para medir la efectividad de la política se podrán establecer indicadores como:

- Número de incidentes de seguridad reportados y gestionados.
- Nivel de cumplimiento de controles de seguridad.
- Porcentaje de equipos actualizados y protegidos.
- Tiempo de respuesta ante incidentes de seguridad.
- Nivel de capacitación en seguridad digital del personal.
- Cumplimiento de planes de tratamiento de riesgos.

3. Responsables del Seguimiento

El proceso de seguimiento y medición estará a cargo del área de Tecnologías de la Información, en coordinación con las dependencias responsables de la gestión institucional, control interno y gestión del riesgo, quienes deberán presentar informes periódicos a la alta dirección.

4. Evaluación y Mejora Continua

Los resultados del seguimiento permitirán identificar oportunidades de mejora, debilidades o riesgos emergentes, con el fin de implementar acciones correctivas y preventivas que fortalezcan la seguridad digital institucional.

La política deberá revisarse y actualizarse periódicamente o cuando se presenten cambios significativos en:

- La normatividad aplicable.
- La infraestructura tecnológica.
- Los riesgos de seguridad digital.
- La estructura organizacional.
- Los procesos institucionales.

5. Reportes e Informes

Se elaborarán informes de seguimiento que permitan evidenciar el cumplimiento de la política, los avances en la implementación de controles, la gestión de incidentes y el estado de los riesgos de seguridad digital, los cuales servirán como insumo para la toma de decisiones institucionales.

6. Auditoría y Control

La institución podrá realizar auditorías de seguridad digital para verificar el cumplimiento de la política y los controles establecidos, conforme a los lineamientos de control interno y las disposiciones legales vigentes.

12. GLOSARIO DE TÉRMINOS

Activo de Información:

Cualquier elemento que tenga valor para la institución y que contenga, procese o soporte información, incluyendo datos, sistemas, equipos, aplicaciones, servicios, infraestructura tecnológica y talento humano.

Amenaza:

Causa potencial de un incidente no deseado que puede generar daño a un sistema, proceso o activo de información.

Autenticación:

Proceso mediante el cual se verifica la identidad de un usuario, sistema o entidad antes de permitir el acceso a recursos tecnológicos.

Confidencialidad:

Propiedad de la información que garantiza que solo esté disponible para personas, entidades o procesos autorizados.

Control de Acceso:

Mecanismos y procedimientos que limitan el acceso a sistemas, aplicaciones o información únicamente a usuarios autorizados.

Copia de Seguridad (Backup):

Proceso de duplicación de la información para garantizar su recuperación en caso de pérdida, daño o incidente de seguridad.

Datos Personales:

Cualquier información vinculada o que pueda asociarse a una persona natural identificada o identificable.

Disponibilidad:

Propiedad de la información que garantiza que esté accesible y utilizable cuando sea requerida por un usuario autorizado.

Gestión de Riesgos:

Proceso para identificar, analizar, evaluar y tratar los riesgos que pueden afectar la seguridad de la información.

Incidente de Seguridad de la Información:

Evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información o los sistemas.

Integridad:

Propiedad de la información que garantiza que sea exacta, completa y no haya sido modificada sin autorización.

Política de Seguridad de la Información:

Conjunto de directrices, normas y lineamientos establecidos para proteger los activos de información de una organización.

Privacidad:

Derecho de las personas a controlar el acceso y uso de su información personal.

Riesgo:

Posibilidad de que una amenaza aproveche una vulnerabilidad y genere un impacto negativo en los activos de información.

Seguridad de la Información:

Conjunto de medidas orientadas a proteger la información contra accesos no autorizados, alteraciones, pérdidas o destrucción.

Seguridad Digital:

Aplicación de estrategias, políticas, controles y tecnologías para proteger los activos digitales y la información en entornos tecnológicos.

Sistema de Información:

Conjunto de recursos organizados para recopilar, procesar, almacenar y distribuir información.

Tecnologías de la Información y las Comunicaciones (TIC):

Herramientas tecnológicas utilizadas para el procesamiento, almacenamiento y transmisión de información.

Usuario:

Persona autorizada que accede a los sistemas de información o recursos tecnológicos de la institución.

Vulnerabilidad:

Debilidad de un activo o control que puede ser explotada por una amenaza para causar un incidente de seguridad.