ACUERDO CONSEJO DIRECTIVO 005
(18 de febrero de 2026)

Por medio del cual se modifica la Política de Seguridad y Privacidad de la Información de la Institución Universitaria Pascual Bravo y se deroga el Acuerdo Directivo 031 de 2021

El Consejo Directivo, en ejercicio de sus atribuciones legales y estatutarias, y en especial de las conferidas en el artículo 15, literales e), g) y t), del Acuerdo 015 del 22 de diciembre de 2017, y

CONSIDERANDO

Que la Ley 1581 de 2012, el Decreto 1078 de 2015 y la Resolución 500 de 2021, entre otras normas, establecen lineamientos para la protección de datos personales, seguridad de la información y gobierno digital en entidades públicas.

Que, el Consejo Directivo en ejercicio de sus funciones legales y en especial de las que le confiere el Artículo 65, literal a, de la Ley 30 de 1992, expide mediante Acuerdo Directivo 015 del 22 de diciembre de 2017, el Estatuto General de la Institución Universitaria Pascual Bravo.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) define el Modelo de Seguridad y Privacidad de la Información (MSPI) como marco obligatorio para la gestión de seguridad y privacidad de la información en entidades públicas.

Que la Institución Universitaria Pascual Bravo reconoce la importancia de sus activos de información para el cumplimiento de su misión institucional y la confianza de la ciudadanía, servidores públicos, docentes, estudiantes, contratistas y demás partes interesadas.

Que es necesario actualizar la política de seguridad y privacidad de la información, incorporando roles, responsabilidades, mecanismos de seguimiento, indicadores, protección de activos críticos y mejora continua conforme al MSPI, apoyado en el SGSI como mecanismo de implementación.

Que la implementación de esta política contribuye a fortalecer la cultura de seguridad de la información, la gestión de riesgos y la eficiencia de los procesos institucionales.

Que en atención a la necesidad de actualizar y unificar la regulación interna sobre la Política de Seguridad y Privacidad de la Información de la Institución

Universitaria Pascual Bravo se hace necesario derogar el Acuerdo Directivo 031 de 2021.

Que en mérito de lo expuesto,

ACUERDA

ARTÍCULO PRIMERO. Modificar la Política de Seguridad y Privacidad de la Información de la Institución Universitaria Pascual Bravo, que se encuentra contenida en su totalidad en los anexos No.1 y No. 2 que hacen parte integral del presente Acuerdo

ARTÍCULO SEGUNDO. Facultar al Rector de la Institución o quien haga sus veces, para que realice todas las acciones, modificaciones y/o trámites necesarios para operativizar o perfeccionar la mencionada política.

ARTÍCULO TERCERO. El presente Acuerdo rige a partir de su publicación y deroga todas las disposiciones contrarias, incluido el Acuerdo Directivo 031 de 2021.

PUBLÍQUESE Y CÚMPLASE

Dado en Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, a los 18 días del mes de febrero de 2026.

Original Firmado
CAROLINA FRANCO GIRALDO
Presidente

Original Firmado
JUAN PABLO MARTÍNEZ RENGIFO
Secretario

Proyectó: Sara Margarita Guzmán Cano Contratista de la Dirección de Planeación y Aseguramiento de la Calidad	Elaboró: Luis Fernando Espinosa Alzate Contratista de la Dirección de Planeación y Aseguramiento de la Calidad	Revisó: Jeannette Gilede Directora de la Dirección de Planeación y Aseguramiento de la Calidad
Firma:	Firma:	Firma:

ANEXO 1.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

INSTITUCIÓN UNIVERSITARIA PASCUAL BRAVO

2026

TABLA DE CONTENIDO

OBJETIVO

Establecer los lineamientos, principios, roles y responsabilidades definidos por la Alta Dirección de la Institución Universitaria Pascual Bravo para la gestión de la Seguridad y Privacidad de la Información, en cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), como marco obligatorio para las entidades públicas, y la normatividad vigente, garantizando la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y privacidad de la información institucional.

DEFINICIONES / GLOSARIO

Para efectos de la presente política se adoptan, entre otros, los siguientes términos:

- **Activo de Información:** Información o elemento que la soporta y que tiene valor para la Institución.
- **Activo Crítico:** Activo de información esencial para el cumplimiento de los procesos institucionales.
- **Confidencialidad:** Propiedad de la información que evita su divulgación a personas, entidades o procesos no autorizados.
- **Integridad:** Propiedad que preserva la exactitud y completitud de la información.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable cuando sea requerida por una parte interesada autorizada.
- **Autenticidad:** Garantía del origen legítimo y confiable de la información.
- **Amenaza:** Causa potencial de un incidente no deseado que puede generar impacto sobre los activos de información.
- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza explote una vulnerabilidad causando impacto sobre los activos de información.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información definido por el Ministerio TIC.
- **SGSI:** Sistema de Gestión de Seguridad de la Información, utilizado como mecanismo para la implementación del MSPI.
- **Ciberseguridad:** Proceso de protección de los activos de información frente a amenazas digitales.
- **Control:** Medida destinada a modificar o reducir un riesgo.

El glosario podrá ampliarse conforme a los documentos complementarios del MSPI.

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Institución Universitaria Pascual Bravo, entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, se compromete con la implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI), como mecanismo de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), orientado a proteger la confidencialidad, integridad, disponibilidad, autenticidad y privacidad de los activos de información.

Lo anterior con el fin de establecer un marco de confianza en el desarrollo de sus funciones misionales, administrativas y académicas frente al Estado, la comunidad educativa y la ciudadanía en general, en estricto cumplimiento de la normatividad legal y reglamentaria aplicable.

En desarrollo de esta política, la Institución establecerá políticas, manuales, procedimientos, instructivos y controles técnicos, administrativos y físicos necesarios para proteger sus activos de información frente a amenazas internas o externas, intencionales o accidentales, garantizando la protección de los derechos de las partes interesadas.

La presente política se complementa con el Manual de Políticas del MSPI y demás documentos derivados que desarrollan de manera específica los lineamientos aquí establecidos.

OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

En coherencia con el Modelo de Seguridad y Privacidad de la Información (MSPI), la Institución Universitaria Pascual Bravo establece los siguientes objetivos, los cuales serán objeto de seguimiento y medición a través del Sistema de Gestión de Seguridad de la Información, apoyado en el SGSI:

- Fortalecer la cultura de seguridad y privacidad de la información en los servidores públicos, docentes, contratistas, estudiantes, practicantes, proveedores y terceros que tengan acceso a información institucional.
- Establecer, implementar y mantener políticas, manuales, procedimientos e instructivos que regulen la gestión de la seguridad y privacidad de la información.
- Identificar, evaluar y minimizar los riesgos de seguridad y privacidad de la información asociados a los procesos institucionales.
- Garantizar el cumplimiento de la normatividad vigente en materia de seguridad de la información, protección de datos personales y gobierno digital.
- Mejorar continuamente la eficacia del Sistema de Gestión de Seguridad de la Información.

COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de la Institución Universitaria Pascual Bravo manifiesta su compromiso con la adopción, implementación, mantenimiento y mejora continua del **Modelo de Seguridad y Privacidad de la Información (MSPI)**, como parte integral del gobierno institucional y del cumplimiento de la Política de Gobierno Digital.

En desarrollo de este compromiso, la Alta Dirección se compromete a:

- Liderar y respaldar la implementación del MSPI, promoviendo una cultura institucional de seguridad y privacidad de la información.
- Garantizar la asignación y disponibilidad de los recursos humanos, técnicos, tecnológicos y financieros necesarios para la implementación y sostenibilidad del MSPI.
- Integrar la seguridad y privacidad de la información en los procesos de planeación estratégica, gestión institucional y toma de decisiones.
- Realizar seguimiento periódico al desempeño, avance y eficacia del MSPI, a través de los mecanismos de evaluación definidos.
- Asegurar el cumplimiento de la normatividad vigente aplicable, en especial la Resolución 500 de 2021, el Decreto 1078 de 2015 y demás disposiciones relacionadas con la seguridad y privacidad de la información.
- Promover la articulación del MSPI con los sistemas de gestión institucionales y los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG).
- Garantizar que las decisiones institucionales incorporen criterios de seguridad y privacidad de la información.

ALCANCE DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

La Institución Universitaria Pascual Bravo implementa el **Modelo de Seguridad y Privacidad de la Información (MSPI)**, conforme a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones y a la normatividad vigente, como marco institucional para la gestión de la seguridad y privacidad de la información.

El alcance del MSPI comprende todos los procesos estratégicos, misionales, de apoyo y de evaluación de la Institución, así como la información en cualquier formato o medio, los activos que la soportan, los sistemas de información, la infraestructura tecnológica, los

servicios digitales y las personas que intervienen en su creación, procesamiento, almacenamiento, transmisión y disposición.

Para efectos de su implementación y mejora continua, el MSPI se operacionaliza a través del Sistema de Gestión de Seguridad de la Información (SGSI), garantizando que las medidas de seguridad y privacidad de la información se apliquen de manera coherente, proporcional y alineada con los riesgos identificados y los objetivos institucionales.

APLICABILIDAD

La presente Política General de Seguridad y Privacidad de la Información establece los lineamientos de obligatorio cumplimiento para todas las personas, procesos y recursos que intervienen en la gestión de la información de la Institución Universitaria Pascual Bravo, en el marco del Modelo de Seguridad y Privacidad de la Información (MSPI) y la normatividad vigente.

En este sentido, la política aplica a:

- Directivos de la Institución Universitaria Pascual Bravo.
- Profesores.
- Funcionarios administrativos.
- Contratistas y proveedores.
- Estudiantes, practicantes y demás terceros que, en razón de su relación con la Institución, accedan, utilicen, administren, procesen, custodien o tengan conocimiento de la información institucional.

Así mismo, la política es aplicable a:

- Todos los procesos estratégicos, misionales, de apoyo y de evaluación de la Institución.
- La información institucional en cualquier formato o medio (físico, digital, electrónico u otro).
- Los activos que soportan la información, incluidos sistemas de información, infraestructura tecnológica, servicios digitales y recursos humanos.
- Todo el ciclo de vida de la información, desde su creación hasta su disposición final.

El incumplimiento de lo establecido en la presente política y en los documentos que de ella se deriven dará lugar a las acciones disciplinarias, administrativas, contractuales o legales a que haya lugar, conforme a la normatividad vigente.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

La Institución Universitaria Pascual Bravo, define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Manuales, Procedimientos, Formatos etc.…):

Rol / Instancia	Responsabilidades
Alta Dirección	Aprobar la política, asignar recursos y liderar el MSPI.
Comité Institucional de Gestión y Desempeño	Hacer seguimiento y apoyar decisiones estratégicas del MSPI.
Oficial de Seguridad de la Información	Coordinar la implementación del MSPI, gestionar los riesgos de seguridad de la información, articular el SGSI como mecanismo de implementación del MSPI, conforme a los lineamientos del Ministerio TIC.
Oficial de Protección de Datos Personales	Velar por el cumplimiento del régimen de protección de datos personales, coordinar la atención de titulares, articularse con el MSPI y asegurar la implementación de los principios de privacidad y protección de datos.
Dirección TIC	Implementar controles tecnológicos y gestionar incidentes.
Talento Humano	Promover la cultura de seguridad y garantizar la capacitación.
Control Interno	Evaluar el cumplimiento del MSPI y apoyar auditorías.
Dirección de Comunicaciones	Apoyar la gestión de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información, incluyendo campañas de sensibilización, divulgación de lineamientos del MSPI y coordinación de comunicaciones oficiales en caso de incidentes de seguridad de la información, conforme a los protocolos definidos por la Institución.
Líderes de Proceso	Aplicar controles y lineamientos del MSPI en sus procesos.
Usuarios de la Información	Cumplir las políticas y proteger los activos de información.

SANCIONES

Las infracciones a la presente política serán sancionadas conforme al Reglamento Interno de Trabajo, contratos vigentes y la normatividad legal aplicable, teniendo en cuenta la gravedad, impacto e intencionalidad del hecho.

SEGUIMIENTO, MEDICIÓN Y MEJORA

La Institución realizará seguimiento periódico al MSPI, apoyado en el SGSI, mediante indicadores, auditorías internas, autoevaluaciones del MSPI y reportes a los entes de control correspondientes.

- Revisión de indicadores definidos para el Sistema de Gestión de Seguridad de la Información.
- Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.
- Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por FURAG o la herramienta definida para tal fin.

APROBACIÓN Y REVISIÓN

La presente Política General de Seguridad y Privacidad de la Información rige a partir de su aprobación por el Consejo Directivo de la Institución Universitaria Pascual Bravo y será de obligatorio cumplimiento para todas las partes interesadas.

La política será revisada y, de ser necesario, actualizada como mínimo una (1) vez al año, o cuando se presenten situaciones que así lo ameriten, tales como:

- Cambios normativos, regulatorios o lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) u otras autoridades competentes.
- Cambios organizacionales, estructurales o funcionales en la Institución (reestructuración de áreas, procesos o responsabilidades).
- Incidentes de seguridad y/o privacidad de la información que evidencien la necesidad de ajustes o mejoras en la política.
- Resultados de auditorías, evaluaciones internas, autoevaluaciones del MSPI o requerimientos de los entes de control.

La revisión de la política permitirá evaluar su efectividad, pertinencia y alineación con los objetivos institucionales y con el Modelo de Seguridad y Privacidad de la Información (MSPI), garantizando su mejora continua.

DOCUMENTOS COMPLEMENTARIOS DEL MSPI

La presente Política General de Seguridad y Privacidad de la Información establece los lineamientos generales y el marco institucional para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la Institución Universitaria Pascual Bravo.

El desarrollo, implementación y operación de estos lineamientos se realiza a través de documentos complementarios, entre los cuales se encuentra el “Manual de Políticas del Modelo de Seguridad y Privacidad de la Información (MSPI)”, en el cual se definen de manera detallada las políticas específicas, controles, responsabilidades y lineamientos técnicos, administrativos y operativos asociados a cada uno de los dominios del MSPI.

El Manual de Políticas MSPI hace parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) como mecanismo de implementación del MSPI y será adoptado, actualizado y administrado por la Institución conforme a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), sin perjuicio de la aprobación de la presente política por parte del Consejo Directivo.

ANEXO 2.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

INSTITUCIÓN UNIVERSITARIA PASCUAL BRAVO

2026

TABLA DE CONTENIDO

1. OBJETIVO DEL MANUAL

Establecer lineamientos relacionados con la seguridad de la información, como complemento de la "Política de Seguridad de la Información de la Institución Universitaria Pascual Bravo", con el fin de preservar la confidencialidad, integridad, disponibilidad, autenticidad y privacidad de los activos de información institucionales, académicos y administrativos, garantizando el cumplimiento normativo y fortaleciendo la cultura de seguridad en toda la entidad.

2. ALCANCE DEL MANUAL

Este manual aplica a todos los funcionarios, contratistas, terceros, proveedores, estudiantes, usuarios y visitantes que interactúen de alguna manera con los activos de información de la Institución Universitaria Pascual Bravo, ya sea de forma física o digital.

3. DEFINICIONES

- **Activo de Información:** Información o elemento que la soporta y que tiene valor para la Institución.
- **Activo Crítico:** Activo de información indispensable para la continuidad de los procesos institucionales.
- **Amenaza:** Causa potencial de un incidente no deseado que puede generar impacto negativo sobre los activos de información.
- **Análisis de Riesgos:** Proceso sistemático para identificar, evaluar y tratar los riesgos de seguridad y privacidad de la información**.**
- **Autenticación:** Proceso para verificar la identidad de un usuario, sistema o entidad.
- **Autorización:** Proceso mediante el cual se conceden permisos de acceso a la información y a los sistemas.
- **Brecha de Seguridad:** Incidente que compromete la confidencialidad, integridad o disponibilidad de la información.
- **Ciberseguridad:** Conjunto de prácticas orientadas a la protección de activos de información frente a amenazas digitales.
- **Clasificación de la Información:** Proceso mediante el cual se asignan niveles de sensibilidad a la información según su impacto.
- **Confidencialidad:** Propiedad que garantiza que la información no sea divulgada a personas no autorizadas.

- **Continuidad del Negocio:** Capacidad de la Institución para continuar la operación de sus procesos críticos ante incidentes disruptivos.
- **Control de Seguridad:** Medida administrativa, técnica o física destinada a reducir un riesgo.
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una persona natural identificada o identificable.
- **Datos Sensibles:** Datos personales que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación.
- **Disponibilidad:** Propiedad de que la información esté accesible y utilizable cuando sea requerida.
- **Gestión de Incidentes de Seguridad:** Proceso para detectar, reportar, analizar y responder a incidentes de seguridad y privacidad de la información.
- **Gestión de Riesgos:** Actividades coordinadas para dirigir y controlar la seguridad de la información frente a riesgos.
- **Integridad:** Propiedad que salvaguarda la exactitud y completitud de la información.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información y las Comunicaciones.
- **SGSI:** Sistema de Gestión de Seguridad de la Información utilizado como mecanismo para la implementación del MSPI.
- **Parte Interesada:** Persona u organización que puede afectar o verse afectada por la seguridad de la información.
- **Privacidad de la Información:** Derecho y principio que protege el tratamiento adecuado de los datos personales.
- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza explote una vulnerabilidad generando impacto.
- **Titular de los Datos**: Persona natural a quien se refieren los datos personales.
- **Tratamiento de Datos Personales:** Cualquier operación sobre datos personales como recolección, almacenamiento, uso o supresión.
- **Usuario de la Información:** Persona autorizada para acceder y utilizar información institucional.
- **Violación de Datos Personales:** Incidente que conlleva la destrucción, pérdida, alteración, divulgación o acceso no autorizado a datos personales.

4. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

4.1. POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

Descripción:

Esta política establece los lineamientos relacionados con la seguridad de la información en la gestión del talento humano. Reconoce que los riesgos asociados a las personas, ya sean funcionarios, contratistas o terceros, son críticos para la protección de los activos de

información de la Institución. Por ello, regula los procesos de selección, inducción, capacitación y responsabilidades del personal, asegurando que quienes tengan acceso a los sistemas y datos institucionales actúen de manera confiable y cumplan con los compromisos de confidencialidad y uso adecuado de los recursos.

Objetivo:

Garantizar que el personal y contratistas cumplan criterios de confiabilidad, formación y conocimiento sobre seguridad de la información, minimizando riesgos internos a los activos de información.

Alcance:

Aplica a todos los funcionarios, contratistas y terceros que tengan acceso a los activos de información de la Institución Universitaria Pascual Bravo.

Lineamientos:

- Verificación de antecedentes disciplinarios de todos los candidatos.
- Firma obligatoria de acuerdos de confidencialidad, privacidad de datos y aceptación de políticas de seguridad.
- Inclusión de políticas de seguridad en inducciones y capacitaciones.

Procedimientos:

- La Dirección de Talento Humano verifica antecedentes antes de la contratación.
- Oficial de Seguridad de la Información coordina la inducción y capacitación en seguridad de la información.

Controles asociados: ISO 27001: A.7.1, A.7.2 / NIST PS-2, PS-3.

Responsables:

- Dirección de Talento Humano: cumplimiento de verificaciones y acuerdos de confidencialidad.
- El proceso de Gestión TIC / Oficial de Seguridad de la Información: capacitación, inducción y seguimiento.

Indicadores:

- % de personal con acuerdos firmados y capacitaciones completadas (Meta: 100% anual).

4.2. POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

Descripción:

La gestión de activos de información asegura que toda información generada, almacenada o procesada en la Institución, ya sea física o digital, sea reconocida como un activo crítico. Esta política define cómo identificar, clasificar, custodiar y proteger estos activos para garantizar su disponibilidad, integridad y confidencialidad, y para que su uso sea estrictamente institucional.

Objetivo:

Proteger los activos de información de la Institución, asegurando su adecuada identificación, custodia y uso conforme a las políticas institucionales.

Alcance:

Aplica a todos los funcionarios, contratistas, terceros y proveedores que manipulen información institucional.

Lineamientos:

- Todos los activos de información son propiedad de la institución.
- Uso de recursos institucionales únicamente para fines laborales.
- Inventario y clasificación de activos de información según criterios de confidencialidad y criticidad.

Procedimientos:

- Registro y actualización periódica del inventario de activos.
- Etiquetado de activos según su nivel de confidencialidad.
- Control periódico de uso y custodia de activos.

Controles asociados: ISO 27001: A.8 / NIST CM-8, MP-4

Responsables:

- El Proceso de Gestión TIC: actualización y custodia del inventario.
- Líderes de Proceso: supervisión del uso adecuado de los activos.

Indicadores:

- % de activos inventariados y clasificados (Meta: 100% anual).

4.3. POLÍTICAS DE CONTROL DE ACCESO LÓGICO

Descripción:

Esta política busca controlar el acceso a la información y los sistemas de la Institución, estableciendo procedimientos para que únicamente personas autorizadas puedan interactuar con los activos de información. Reconoce que los accesos indebidos son uno de los riesgos principales para la confidencialidad e integridad de la información.

Objetivo:

Prevenir accesos no autorizados y proteger la confidencialidad, integridad y disponibilidad de los activos de información institucionales.

Alcance:

Aplica a todos los usuarios que tengan acceso a sistemas, redes y datos institucionales.

Lineamientos:

- Cada usuario tendrá credenciales personales e intransferibles.
- Se recomienda la activación de autenticación multifactor (MFA).
- Las cuentas inactivas deben deshabilitarse dentro de las 24 horas.
- Uso responsable de la información a la que se accede.

Procedimientos:

- Creación y asignación de usuarios y contraseñas por el Proceso de Gestión TIC.
- Revisión periódica de accesos y revocación de cuentas según necesidad.

Controles asociados: ISO 27001: A.9, A.12 / NIST AC-2, IA-5

Responsables:

- El Proceso de Gestión TIC: administración de accesos y seguimiento de credenciales.
- Dirección de Planeación y Aseguramiento de la Calidad: auditoría de cumplimiento de accesos.

Indicadores:

- % de cuentas revisadas y conformes (Meta: 100% trimestral).

4.4. POLÍTICAS DE CRIPTOGRAFÍA

Descripción:

Establece los lineamientos para el uso de cifrado en la protección de la información digital, garantizando la confidencialidad e integridad de los datos. Incluye la identificación de equipos y sistemas que requieren controles criptográficos adicionales según el nivel de riesgo y criticidad de la información.

Objetivo:

Proteger la confidencialidad e integridad de la información mediante el uso de técnicas criptográficas apropiadas.

Alcance:

Aplica a todos los sistemas, dispositivos y comunicaciones institucionales que manejen información crítica o sensible.

Lineamientos y procedimientos:

- Implementación de cifrado en datos sensibles y comunicaciones.
- Instalación de controles criptográficos adicionales en sistemas de alto riesgo.
- Revisión periódica de algoritmos y claves de cifrado.

Controles asociados: ISO 27001: A.10 / NIST SC-12, SC-13.

Responsables:

- El Proceso de Gestión TIC: configuración y mantenimiento de cifrado.
- Oficial de Seguridad de la Información: supervisión y auditoría.

Indicadores:

- % de sistemas críticos con cifrado activo (Meta: 100%).

4.5. POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

Descripción:

Esta política regula el acceso físico a las instalaciones y áreas críticas de la Institución, garantizando que los activos de información y los recursos tecnológicos se encuentren protegidos frente a riesgos de robo, daño, acceso no autorizado, desastres o condiciones ambientales adversas. Busca que las instalaciones funcionen como un entorno seguro y controlado para la operación académica y administrativa.

Objetivo:

Prevenir riesgos físicos que puedan afectar la confidencialidad, integridad o disponibilidad de los activos de información.

Alcance:

Aplica a todos los funcionarios, contratistas, proveedores, visitantes y terceros que ingresen a las instalaciones institucionales.

Lineamientos y procedimientos:

- Definir áreas seguras con controles de acceso físico.
- Implementar controles ambientales (temperatura, humedad, alarmas, cámaras).
- Registro de visitantes y control de acceso temporal.
- Supervisión periódica de cerraduras, sistemas de alarma y CCTV.

Controles asociados: ISO 27001: A.11 / NIST PE-3, PE-6

Responsables:

- El Proceso de Gestión TIC y Seguridad Física: administración y monitoreo de controles.
- La Vicerrectoría Administrativa y Financiera: supervisión del cumplimiento de accesos y seguridad física.

Indicadores:

- % de áreas seguras con controles activos (Meta: 100%).
- Número de incidentes físicos reportados vs. mitigados.

4.6. POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

Descripción:

Esta política asegura que las operaciones de los sistemas y servicios tecnológicos se realicen de forma segura, controlada y confiable, minimizando riesgos de interrupciones o fallas que afecten la misión académica y administrativa.

Objetivo:

Proteger la operación tecnológica y los servicios institucionales, asegurando disponibilidad, integridad y confidencialidad de la información.

Alcance:

Aplica a todos los sistemas, plataformas, aplicaciones y recursos tecnológicos utilizados por la institución.

Lineamientos y procedimientos:

- Monitoreo continuo de sistemas y redes.
- Procedimientos de respaldo periódico y recuperación ante fallas.
- Gestión de cambios con evaluación de riesgos antes de su implementación.
- Aplicación de controles de seguridad de acuerdo con los procedimientos del SGSI.

Controles asociados: ISO 27001: A.12 / NIST CM-3, CP-9

Responsables:

- El Proceso de Gestión TIC: operación, mantenimiento, monitoreo y soporte técnico.
- Líderes de proceso: supervisión de continuidad operativa.

Indicadores:

- % de disponibilidad de sistemas críticos (Meta: ≥99%).
- Número de incidentes operativos mitigados.

4.7. POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES

Descripción:

Esta política establece controles para proteger la información que circula dentro y fuera de

la institución, asegurando que la transmisión de datos se realice de manera segura, evitando interceptaciones, fugas de información o alteraciones.

Objetivo:

Garantizar la seguridad y confidencialidad de la información en tránsito y asegurar la integridad de las comunicaciones institucionales.

Alcance:

Aplica a todas las redes, servicios de correo electrónico, comunicaciones internas y externas, y transferencias de información institucional.

Lineamientos y procedimientos:

- Implementar controles de seguridad en redes y comunicaciones.
- Encriptación de información sensible en tránsito.
- Uso de canales oficiales para transferencia de información.
- Monitoreo y auditoría de tráfico de red ante incidentes.
-

Controles asociados: ISO 27001: A.13 / NIST SC-12, SC-28

Responsables:

- El Proceso de Gestión TIC: configuración de redes, monitoreo y auditoría.
- Oficial de Seguridad de la Información: supervisión de cumplimiento y reporte de incidentes.

Indicadores:

- % de comunicaciones críticas cifradas (Meta: 100%).
- Número de incidentes de comunicaciones detectados y mitigados.

4.8. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Descripción:

Esta política regula la adquisición, desarrollo, implementación y mantenimiento de sistemas de información, asegurando que cumplan con los estándares de seguridad y buenas prácticas institucionales. Busca integrar la seguridad desde el diseño hasta la operación continua de los sistemas.

Objetivo:

Garantizar que todos los sistemas cumplan con los requisitos de seguridad y buenas prácticas, reduciendo riesgos asociados a fallas o vulnerabilidades.

Alcance:

Aplica a todos los sistemas de información adquiridos, desarrollados o mantenidos por la institución.

Lineamientos y procedimientos:

- Revisión de requisitos de seguridad antes de la adquisición o desarrollo.
- Implementación de metodologías seguras en desarrollo y mantenimiento.
- Informar el Proceso de Gestión TIC sobre proyectos tecnológicos para evaluación de riesgos.
- Actualización de sistemas según políticas de seguridad.

Controles asociados: ISO 27001: A.14 / NIST SA-11, SA-12

Responsables:

- El Proceso de Gestión TIC: evaluación técnica, supervisión y mantenimiento.
- Líderes de procesos: comunicación de necesidades y seguimiento de cumplimiento.

Indicadores:

- % de proyectos con evaluación de seguridad previa (Meta: 100%).
- Número de vulnerabilidades identificadas y mitigadas en sistemas implementados.

4.9. POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

Descripción:

Esta política establece criterios de seguridad de la información en la gestión de proveedores, garantizando que los terceros que presten servicios o suministren sistemas cumplan con los estándares institucionales de protección de información.

Objetivo:

Reducir riesgos asociados a proveedores y garantizar la confidencialidad, integridad y disponibilidad de la información compartida.

Alcance:

Aplica a todos los contratos y relaciones con proveedores, contratistas y terceros que tengan acceso a información institucional.

Lineamientos y procedimientos:

- Suscripción de acuerdos de confidencialidad y seguridad antes de iniciar la relación contractual.
- Evaluación de riesgos de proveedores que manejan información crítica.
- Supervisión y auditoría periódica del cumplimiento de los requisitos de seguridad.

Controles asociados: ISO 27001: A.15 / NIST SA-9, SA-10

Responsables:

- Dirección Jurídica: gestión de acuerdos y revisión de contratos.
- El Proceso de Gestión TIC: seguimiento y auditoría de proveedores.

Indicadores:

- % de proveedores con acuerdos de confidencialidad activos (Meta: 100%).
- Número de incidentes relacionados con proveedores.

4.10. POLÍTICAS DE SEGURIDAD EN LA CONTINUIDAD DE NEGOCIO

Descripción:

Esta política asegura que los procesos críticos de la Institución puedan continuar operando ante cualquier evento adverso, garantizando la restauración oportuna de servicios tecnológicos y la protección de la información institucional. Incluye planes de contingencia, recuperación de desastres y pruebas periódicas de eficacia.

Objetivo:

Asegurar la continuidad de las operaciones y servicios institucionales, minimizando el impacto de interrupciones y garantizando la seguridad de la información.

Alcance:
Aplica a todos los procesos, sistemas, aplicaciones y servicios críticos de la institución.

Lineamientos y procedimientos:

- Desarrollo de Planes de Continuidad Tecnológica y Planes de Recuperación ante Desastres (DRP).
- Realización de análisis de impacto al negocio (BIA) para identificar procesos críticos.
- Ejecución de pruebas periódicas de continuidad, incluyendo:
  - Pruebas de listas de verificación.
  - Simulacros de contingencia.
- Actualización y documentación de los planes según resultados de pruebas y lecciones aprendidas.

Controles asociados: ISO 27001: A.17 / NIST CP-2, CP-4, CP-6

Responsables:

- El Proceso de Gestión TIC: elaboración, ejecución y actualización del plan.
- Líderes de procesos: soporte y participación en simulacros y pruebas.
- Dirección de Planeación y Aseguramiento de la Calidad: seguimiento de indicadores y mejoras continuas.

Indicadores:

- % de procesos críticos con plan de continuidad actualizado (Meta: 100%).
- Número de pruebas de continuidad realizadas vs. planificadas.

4.11. POLÍTICAS DE GESTIÓN DE INCIDENTES

Descripción:

Esta política establece los lineamientos para identificar, registrar, clasificar, gestionar y resolver incidentes de seguridad de la información o tecnológicos. Busca garantizar una respuesta ágil, reducir el impacto de los incidentes y fortalecer la capacidad de prevención mediante lecciones aprendidas.

Objetivo:

Detectar, atender y resolver oportunamente incidentes tecnológicos y de seguridad, preservando la confidencialidad, integridad y disponibilidad de la información.

Alcance:

Aplica a todos los usuarios, funcionarios, contratistas, proveedores y terceros que interactúen con sistemas y servicios institucionales.

Lineamientos y procedimientos:

- Canal único de atención: Mesa de Ayuda (tickets web, correo institucional, línea autorizada, presencial documentado).
- Registro de incidentes: fecha, tipo, usuario afectado, sistema, impacto, evidencia inicial.
- Clasificación y priorización por impacto, urgencia y tipo (Phishing, Malware, Fuga de información, Falla operativa, etc.).
- Escalamiento de incidentes críticos a responsable TIC, Equipo de Seguridad y Comité Institucional de Seguridad y Privacidad.
- Documentación completa: acciones, evidencias, comunicaciones, análisis y lecciones aprendidas.
- En caso de afectación de datos personales: notificación a la Superintendencia de Industria y Comercio (Ley 1581 de 2012) y a los titulares afectados.

Controles asociados: ISO 27001: A.16 / NIST IR-4, IR-6, IR-8

Responsables:

- Mesa de Ayuda: registro inicial, clasificación, primeros tiempos de respuesta (SLA).
- Equipo de Seguridad de la Información: análisis de causa raíz, contención y escalamiento.
- Dirección Jurídica: soporte legal y reporte ante SIC si aplica.
- Comité Institucional de Seguridad y Privacidad: revisión de informes y aprobación de planes de acción.

Indicadores:

- Tiempo promedio de resolución de incidentes vs SLA.
- Número de incidentes recurrentes por tipo.

4.12. POLÍTICAS DE CUMPLIMIENTO Y USO DE RECURSOS

a) ESCRITORIO LIMPIO

Descripción:

Establece lineamientos para proteger la información física y digital, evitando accesos no autorizados y exposición de datos sensibles.

Objetivo:

Reducir riesgos de pérdida o acceso no autorizado a la información institucional.

Alcance:

Aplica a todos los funcionarios, contratistas y terceros.

Lineamientos:

- Documentos físicos: archivar bajo llave, retirar documentos de impresora, destrucción segura.
- Entorno digital: no almacenar información sensible en escritorio del equipo sin protección, bloquear sesión al ausentarse, cerrar aplicaciones y portales no utilizados.
- Custodia de dispositivos: proteger laptops, móviles y equipos de robo o manipulación.

Controles asociados: ISO 27001: A.7.7, A.8.1 / NIST PE-18, AC-11

Responsables:

- Todos los usuarios con acceso a información institucional.
- El Proceso de Gestión TIC: seguimiento y auditoría de cumplimiento.

Indicadores:

- % de auditorías con cumplimiento total de escritorio limpio (Meta: 100%).

b) USO ADECUADO DE INTERNET

Descripción:

Define criterios para el uso seguro de la red institucional, priorizando la productividad y evitando riesgos de malware, fuga de información o contenido inapropiado.

Objetivo:

Garantizar el uso seguro y adecuado del Internet institucional.

Alcance:

Todos los usuarios de redes y servicios de la institución.

Lineamientos:

- Restringir acceso a sitios de juegos, pornografía, drogas, hacking, torrents o software ilegal.

- Limitar redes sociales salvo uso justificado por labores institucionales.
- Uso exclusivo de la nube institucional para información corporativa.
- Monitoreo de logs de navegación para auditorías o investigaciones.

Controles asociados: ISO 27001: A.5.26, A.8.23 / NIST SC-7, SC-18

Responsables:

- El Proceso de Gestión TIC: monitoreo y aplicación de controles.

Indicadores:

- % de usuarios cumpliendo con políticas de navegación (Meta: 100%).

c) USO ADECUADO DE CORREO ELECTRÓNICO

Descripción:

Establece lineamientos para el uso seguro del correo institucional, previniendo ataques de phishing, malware y fuga de información.

Objetivo:

Proteger la información institucional y garantizar la trazabilidad de los mensajes.

Alcance:

Todos los usuarios con correo institucional.

Lineamientos:

- Uso exclusivo para actividades institucionales.
- Prohibido enviar información institucional a cuentas personales.
- Obligatorio reportar correos sospechosos.
- La oficina TIC puede auditar buzones por continuidad, seguridad o requerimientos legales.

Controles asociados: ISO 27001: A.5.10, A.5.23, A.8.24 / NIST SC-8, SI-8

Responsables:

- El Proceso de Gestión TIC: monitoreo y auditoría.
- Usuarios: uso responsable y reporte de incidencias.

Indicadores:

- Número de incidentes de correo reportados y mitigados.

d) USO DE USUARIOS Y CONTRASEÑAS

Descripción:

Regula la gestión de identidades digitales, asegurando accesos personales, robustos y seguros a los sistemas institucionales.

Objetivo:

Prevenir accesos no autorizados y proteger la información institucional.

Alcance:

Todos los usuarios con acceso a sistemas y servicios TIC.

Lineamientos:

- Credenciales personales, únicas e intransferibles.
- Contraseñas robustas (mayúsculas, minúsculas, números, caracteres especiales, mínimo 12).
- Activar autenticación multifactor (MFA) cuando esté disponible.
- Cambiar contraseña ante sospecha de compromiso.
- Deshabilitación de usuarios inactivos en 24h.
- Uso de cuentas privilegiadas solo para tareas administrativas autorizadas.

Controles asociados: ISO 27001: A.5.17, A.5.18 / NIST IA-5, AC-2

Responsables:

- Dirección de Planeación y Aseguramiento de la Calidad: seguimiento.
- El Proceso de Gestión TIC: administración de cuentas y auditorías.
- Todos los usuarios: cumplimiento de lineamientos.

Indicadores:

- % de cuentas con MFA activo (Meta: 100%).
- Número de incidentes por mal uso de credenciales.

5. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Descripción:

Se establecen estrategias para socializar las políticas de seguridad y promover la cultura de protección de información en toda la institución.

Objetivo:

Fortalecer la cultura de seguridad de la información, fomentando comportamientos seguros y cumplimiento de políticas.

Alcance:

Todos los funcionarios, contratistas, proveedores y terceros de la institución.

Lineamientos:

- Plan anual de Sencibilizaciones de buenas prácticas.
- Inclusión de seguridad de la información en inducciones y capacitaciones.
- Identificación de perfiles de conocimiento y públicos objetivos.
- Medición de resultados de capacitación y apropiación de políticas.

Responsables:

- Dirección de Talento Humano: inclusión en capacitaciones e inducciones.
- El Proceso de Gestión TIC y Oficial de Seguridad: elaboración de contenidos y seguimiento.

Indicadores:

- % de usuarios capacitados (Meta: 100%).
- Resultados de encuestas de conocimiento sobre seguridad.

6. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Descripción:

Establece la formalización, vigencia y actualización de las políticas de Seguridad y Privacidad de la información.

Objetivo:

Garantizar la vigencia, aplicabilidad y adaptación de las políticas a cambios tecnológicos y de riesgos.

Alcance:

Todas las políticas contenidas en el manual.

Lineamientos:

- Aprobación por Alta Dirección.
- Revisión mínima anual o ante incidentes graves o cambios estructurales.
- Registro formal de versiones y cambios.

Responsables:

- Alta Dirección: aprobación y seguimiento.
- Comité Institucional de Seguridad y Privacidad de la Información: revisión y ajustes.

Indicadores:

- Cumplimiento de calendario de revisiones (Meta: 100%).

7. SANCIONES

Descripción:

Define las consecuencias por incumplimiento de las Políticas de Seguridad y Privacidad de la información.

Objetivo:

Garantizar responsabilidad, disciplina y cumplimiento de las políticas institucionales.

Alcance:

Todos los funcionarios, contratistas, proveedores y terceros.

Lineamientos:

- Aplicación de sanciones según Código Único Disciplinario.
- Posibles sanciones penales según gravedad y determinación de autoridades competentes.
- El Proceso de Gestión TIC entrega evidencias a la Oficina de Control Disciplinario y registra incidentes de seguridad derivados del incumplimiento.

Responsables:

- El Proceso de Gestión TIC: recopilación de evidencias y gestión de incidentes.
- Oficina de Control Disciplinario: determinación de sanciones.

Indicadores:

- Número de sanciones aplicadas por incumplimiento.
- Tiempo promedio de resolución de incidentes disciplinarios.

El presente Manual de Políticas del Modelo de Seguridad y Privacidad de la Información (MSPI) hace parte integral del acto administrativo mediante el cual la Institución Universitaria Pascual Bravo adopta la Política de Seguridad y Privacidad de la Información y el MSPI, y constituye el documento técnico que desarrolla, complementa y operacionaliza los lineamientos allí definidos.