

|                                                                         |                                    |                                                                              |                                                               |
|-------------------------------------------------------------------------|------------------------------------|------------------------------------------------------------------------------|---------------------------------------------------------------|
| <b>PROCESO:</b><br><i>Gestión de la tecnología e innovación digital</i> | <b>POLÍTICA</b>                    | <b>Acuerdo - Resolución:</b><br><i>Acta No. 356 del Consejo de Delegados</i> | <b>Código:</b><br><i>Registrado por el sistema integrado</i>  |
|                                                                         | <b>SEGURIDAD DE LA INFORMACIÓN</b> | <b>Fecha aprobación:</b><br><i>Agosto 20 de 2026</i>                         | <b>Versión:</b><br><i>Registrado por el sistema integrado</i> |

## 1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

## 2. MARCO LEGAL

### 2.1 MARCO NORMATIVO EXTERNO

La presente Política se desarrolla de conformidad con la Constitución Política de Colombia, las disposiciones legales y reglamentarias aplicables a la protección de la información, datos personales, privacidad, seguridad digital, ciberseguridad, derechos de autor, gestión documental, tecnologías de la información y demás materias relacionadas con la gestión y protección de los activos de información institucionales.

Dentro del marco normativo aplicable se consideran, entre otras, las siguientes disposiciones:

- Constitución Política de Colombia, especialmente los artículos 15 y 20.
- Ley 23 de 1982 y las disposiciones que la modifiquen, adicionen o sustituyan, en materia de derechos de autor y propiedad intelectual.
- Ley 527 de 1999, sobre mensajes de datos, comercio electrónico y firmas digitales.
- Ley 594 de 2000, Ley General de Archivos, en lo que resulte aplicable.
- Ley 1266 de 2008, sobre disposiciones generales del hábeas data, en el ámbito de aplicación correspondiente.
- Ley 1273 de 2009, por medio de la cual se modifica el Código Penal y se establece la protección de la información y los datos.
- Ley 1341 de 2009 y sus modificaciones, en materia de tecnologías de la información y las comunicaciones.
- Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014, sobre transparencia y derecho de acceso a la información pública, en lo que resulte aplicable.
- Decreto 1074 de 2015, en las disposiciones relacionadas con la protección de datos personales.
- Ley 1928 de 2018, por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia, adoptado en Budapest.
- Las demás disposiciones legales y reglamentarias que resulten aplicables a la Institución y que modifiquen, adicionen, sustituyan o desarrollen las anteriormente señaladas.

### 2.2 MARCO NORMATIVO INTERNO

La presente Política se articula con los documentos institucionales vigentes que regulan la gestión, protección y uso de la información, entre ellos:

- Política de Tratamiento y Protección de Datos Personales.
- Política de Gestión de Datos.
- Código de Buen Gobierno.
- Reglamento Interno de Trabajo.
- Reglamento Académico.
- Pacto de Honor Gran Colombiano.
- Política de Gestión de Riesgos.
- Procedimiento de Gestión de Activos de Información.

“Este documento es propiedad intelectual del POLITECNICO GRANCOLOMBIANO, se prohíbe su reproducción total o parcial sin la autorización escrita de la Rectoría. TODO DOCUMENTO IMPRESO O DESCARGADO DEL SISTEMA, ES CONSIDERADO COPIA NO CONTROLADA”.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b><br><i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|---------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b><br><i>Registrado por secretaría general</i>  | <b>Versión:</b><br><i>Registrado por el sistema integrado</i> |

- Procedimiento de Gestión de Incidentes de Seguridad de la Información.
- Procedimientos, manuales, estándares y protocolos relacionados con seguridad de la información y ciberseguridad.
- Lineamientos institucionales relacionados con tecnología, infraestructura, servicios en la nube, gestión de accesos, continuidad y proveedores.
- Contratos y acuerdos de confidencialidad u otros instrumentos que establezcan obligaciones relacionadas con la seguridad de la información.
- Los demás documentos internos que resulten aplicables.

### 3. MARCO TEÓRICO

La Seguridad de la Información comprende el conjunto de principios, políticas, procesos, procedimientos, controles y medidas destinados a proteger la información y los activos asociados a esta frente a amenazas internas o externas, accidentales o intencionales, durante todo su ciclo de vida.

La gestión de la Seguridad de la Información se desarrolla mediante un enfoque basado en riesgos, orientado a identificar, analizar, valorar, tratar, monitorear y comunicar los riesgos que puedan afectar los activos de información, los procesos, los servicios y los objetivos institucionales.

El Sistema de Gestión de Seguridad de la Información –SGSI– constituye el marco de gestión mediante el cual la Institución establece, implementa, mantiene y mejora los procesos y controles destinados a gestionar los riesgos relacionados con la seguridad de la información.

La Ciberseguridad constituye un componente de la Seguridad de la Información orientado a la prevención, protección, detección, respuesta y recuperación frente a amenazas que puedan afectar los sistemas, redes, dispositivos, aplicaciones, servicios y datos en entornos digitales.

La gestión de la Seguridad de la Información se fundamenta principalmente en la preservación de la confidencialidad, integridad y disponibilidad de la información, complementada con la gestión de la privacidad, autenticidad, trazabilidad, responsabilidad, continuidad y demás propiedades de seguridad que resulten aplicables según la naturaleza y criticidad de los activos y procesos institucionales.

#### 3.1 CONCEPTOS

- **Activo de información:** Información, datos, sistemas, aplicaciones, infraestructura tecnológica, servicios, documentos, procesos, personas y cualquier otro recurso que tenga valor para la Institución y requiera protección.
- **Alcance de la auditoria:** Extensión y límites de una auditoria para el SGSI.
- **Amenaza:** Causa potencial de un incidente no deseado que puede ocasionar daños a los activos de información.
- **Análisis Forense:** Actividad que se ejecuta para recabar evidencia de un posible mal uso de los activos de información, el cual haya podido generar fraudes o daños a la reputación de la Institución. Se realiza mediante técnicas especializadas, donde las evidencias pueden ser consideradas para procesos legales.
- **Auditado:** Proceso, procedimiento, servicio o requisito al que se le aplica la auditoria. Para el sistema de gestión el auditado se define de acuerdo con la estructura de la auditoria programada.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- **Auditor ISO27001:** Persona que por su experiencia o conocimiento lidera una auditoria del SGSI. Tiene autonomía para preparar la ejecución de la auditoria, conciliar con los auditados, liderar las reuniones de apertura y cierre de auditorías, actuar en el esclarecimiento de eventuales dudas que surjan durante la ejecución de la auditoría y en la solución de posibles problemas.
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencia del cumplimiento de requisitos, por el cual se evalúa objetivamente la medida en la cual se cumplen los criterios de auditoría.
- **Buzón de Correo:** Corresponde al repositorio local o en servidor donde se localizan los correos electrónicos de una persona o empleado.
- **Ciberseguridad:** Conjunto de prácticas, controles y tecnologías orientadas a proteger sistemas, redes e información frente a amenazas digitales.
- **Cifrar:** Codificar el contenido de un mensaje o archivo para que llegue solamente a la persona autorizada de recibirlo.
- **Código malicioso:** Programas potencialmente peligrosos diseñados para comprometer la seguridad de la información.
- **Confidencialidad de la Información:** Sistemas, medidas o condiciones implementadas por la Institución para preservar la seguridad, disponibilidad e integridad de la información, de conformidad con las restricciones o limitantes que el Politécnico Grancolombiano, sus entes reguladores y el desarrollo mismo de su objeto social han fijado para autorizar el acceso y la divulgación, así como los medios para la protección de la intimidad personal y propiedad de la información.
- **Conformidad:** Cumplimiento de un requisito.
- **Control de acceso:** Mecanismos que limitan la disponibilidad de información o recursos de procesamiento de información solamente a las personas o aplicaciones autorizadas.
- **Control de versión:** Gestión de los diversos cambios que se realizan sobre los elementos de algún producto o una configuración del mismo.
- **Cookies:** Archivo creado por un sitio web que contiene pequeñas cantidades de datos y que se envían entre un emisor y un receptor.
- **Correo Electrónico:** Herramienta de comunicación que permite intercambiar mensajes de texto y archivos adjuntos entre los equipos de la red de datos e Internet.
- **Criterios de Auditoria:** Conjunto de políticas, procedimientos o requisitos utilizados como referencia en la verificación y sobre el cual se evalúa el cumplimiento.
- **Cuenta de usuario de una aplicación:** Asignación de un usuario a un tercero (empleado, estudiante, graduado) para tener acceso a un sistema de aplicación (aplicativo). Tiene un nombre de usuario y una contraseña.

|                                                           |                             |                                                                       |                                                            |
|-----------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | <b>POLÍTICA</b>             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|                                                           | <b>NOMBRE DEL DOCUMENTO</b> | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- **Cuenta de usuario de Windows:** Asignación de un usuario a un tercero (empleado, estudiante, graduado) para tener acceso a un computador de la red de datos de la Institución, que tenga sistema operativo Windows. Tiene un nombre de usuario y una contraseña.
- **Disclaimer:** Advertencias (warnings) unilaterales dirigidas al público en general.
- **Disponibilidad de la información:** Propiedad de la información que garantiza que esta sea accesible y utilizable por las personas autorizadas cuando sea requerida.
- **Equipo auditor:** Persona o grupo de personas que llevan a cabo una auditoria. El equipo auditor se conformará de acuerdo con la estructura de la auditoría programada y puede incluir auditores, y/o expertos técnicos si se requieren. A un auditor del equipo se le designa como líder de este.
- **Evidencia de Auditoria:** Registros, declaraciones de hechos o cualquier otra información presentada por el auditado y/o recolectada para la verificación de los criterios de auditoría.
- **Hash:** Algoritmos que consiguen crear a partir de una entrada una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado. Su propósito es asegurar que no se ha modificado un archivo en una transmisión, hacer ilegible una contraseña o firmar digitalmente un documento.
- **Integridad de la Información:** Propiedad de la información que garantiza su exactitud, completitud y protección frente a modificaciones no autorizadas.
- **Inteligencia Artificial:** Tecnologías capaces de realizar tareas que normalmente requieren capacidades humanas como análisis, generación de contenido o automatización.
- **Intranet:** Sistema de comunicación interactivo mediante el cual se puede emitir, recibir y compartir información de interés general.
- **Inyecciones de código:** Sintaxis para introducir comandos de manera ilícita que permitan leer o modificar la base de datos, comprometiendo el contenido de la consulta original.
- **Incidente de Seguridad:** Evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información.
- **Legislación Colombiana:** Ordenamiento jurídico o conjunto de normas que rige el territorio nacional.
- **Log:** Registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.
- **Medios de almacenamiento extraíbles:** Dispositivos para guardar y portar información de forma electrónica tales como disquetes, CD's, DVD's, discos ZIP, discos ópticos, discos duros externos, memoria digital USB.
- **Mitigación de riesgos:** Mecanismos o acciones que ayudan a administrar el riesgo y permiten reducir el impacto y/o la probabilidad de ocurrencia en caso de que este se materialice.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- **Niveles de riesgos tolerables:** Impacto que la Institución está dispuesta a tolerar en caso de materializarse un riesgo.
- **Normatividad:** Conjunto de políticas, procedimientos, estándares o lineamientos emitidos por la Institución o por diferentes fuentes internas o externas, que enmarcan o rigen el desarrollo de los procesos de la Institución.
- **Open Web Application Security Project (OWASP):** Proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.
- **Periférico:** Elemento o dispositivo del computador que no hace parte de la unidad central, tales como el monitor, mouse, teclado, parlantes, impresora, escáner, unidades de almacenamiento.
- **Phishing:** Técnica de fraude digital utilizada para obtener información confidencial mediante engaño.
- **Política de Seguridad de la Información:** Conjunto de orientaciones generales sobre los cuales deben asentarse todas las definiciones y acciones de seguridad frente al manejo de la información.
- **Principios de seguridad de la información:** Fundamento o regla requerida por la Institución para la debida ejecución de la seguridad de la información.
- **Privilegio:** Niveles de acceso y procesamiento a la información. Ejemplo: consulta, modificación, administración.
- **Propiedad intelectual:** Rama del derecho que protege la producción intelectual a través del reconocimiento de derechos de carácter temporal y con facultades de disposición y explotación económica. Las legislaciones incluyen dentro de la propiedad intelectual la protección de nuevas creaciones y signos distintivos (propiedad industrial) así como la protección de obras artísticas, literarias y científicas (derecho de autor).
- **Pruebas de Penetración:** Práctica realizada para detectar vulnerabilidades que terceros pueden aprovechar, las cuales resultan de fallas en el software, configuraciones inapropiadas. Se pueden realizar de forma remota o local y se ejecutan tal y como lo intentaría un intruso con propósitos adversos para la Institución.
- **Publicar:** Acto mediante el cual se divulga información, esta puede ser confidencial, sensible o privada.
- **Puertas traseras:** Secuencia especial dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo (autenticación) para acceder al sistema.
- **Riesgo:** Efecto de la incertidumbre sobre el cumplimiento de los objetivos institucionales del Politécnico Grancolombiano, derivado de la probabilidad de ocurrencia de una amenaza y de su impacto sobre los activos de información. Para efectos de la presente política, los objetivos institucionales comprenden, entre otros, la alta calidad académica, la inclusión y proyección social, la sostenibilidad financiera, la experiencia de valor para la comunidad educativa y el fortalecimiento de la arquitectura tecnológica institucional.
- **Seguridad de la Información:** Protección de la información y los sistemas de información del acceso no autorizado, la divulgación, la alteración, la modificación o destrucción. La gestión de la seguridad de la información se apoya en el cumplimiento de tres criterios:
  - La confidencialidad

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- La disponibilidad
- La integridad
- **Sistema operativo:** Programa de computador que organiza y gestiona todas las actividades que sobre él se ejecutan. Algunos sistemas operativos son Windows, Unix y Linux.
- **Software Libre:** Software donde los usuarios tienen la libertad para ejecutar, copiar, distribuir, estudiar, modificar o mejorar el software. Se pueden encontrar diferentes distribuciones como shareware, el cual cobra un monto de dinero para poder utilizar el software completamente y GNU que se caracteriza por ser compatible con UNIX.
- **Spam:** Correo electrónico basura (en inglés también conocido como junk-mail o Spam), sobre el cual puede haber copias del mismo mensaje con fines publicitarios o comerciales.
- **Teletrabajo:** Forma de organización laboral, que consiste en el desempeño de actividades remuneradas o en la prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.
- **Usuario líder del sistema:** Usuario de un sistema de información con conocimientos expertos de su funcionalidad y con amplio conocimiento o experiencia de los procesos del área en la cual se desempeña, en algunos casos puede ser el administrador del sistema.
- **Usuario:** Individuo que tiene autoridad limitada y específica otorgada por el dueño/responsable de la información para consultarla, modificarla, adicionarla, divulgarla o eliminarla (mediante los accesos y privilegios otorgados). Dentro de este concepto están incluidos los empleados, contratistas, terceros, clientes, entes internos y externos de control y empresas que tengan alguna relación comercial o estratégica, y que accedan ya sea interna o externamente a cualquier información de la Institución.
- **Virtual Private Network (VPN):** Tecnología que permite la extensión de una red privada como la de la Institución, en un espacio de red pública pero protegida por un canal virtual. Para los empleados es de vital importancia, debido a las tareas adicionales que se tienen que hacer fuera del horario laboral, para teletrabajo y zonas en las que no hay un canal dedicado asignado.

## 4. POLÍTICA

### 4.1 PRINCIPIOS Y VALORES INSTITUCIONALES

La Política de Seguridad de la Información y Ciberseguridad se desarrolla en armonía con los principios y valores institucionales aplicables, especialmente aquellos relacionados con:

- Responsabilidad.
- Integridad.
- Respeto.
- Transparencia.
- Confidencialidad.
- Gestión responsable de la información.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- Cumplimiento.
- Mejora continua.

Estos principios orientan las actuaciones de quienes, en desarrollo de sus funciones, actividades académicas, contractuales o institucionales, tengan acceso a información o activos de información del Politécnico Gran Colombiano.

## 4.2 DECLARACIÓN

- La información es considerada para la Institución como un activo productivo y como tal, hace parte fundamental de la operación diaria, convirtiéndose en un componente esencial e imprescindible que debe ser protegido para el cumplimiento de sus objetivos estratégicos. Este aspecto hace que todos aquellos a quienes se le haya autorizado el acceso a la información, serán responsables por el buen uso que se le dé a la misma.
- Las personas involucradas y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de la Institución, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad y disponibilidad de la información.
- La Dirección de Gobierno Digital es la responsable de difundir a las personas involucradas y vinculadas con la Institución para que cumplan con la Política de Seguridad de la Información, lineamientos y procedimientos establecidos.
- Los estudiantes, empleados, contratistas y cualquier persona natural o jurídica que mantenga un vínculo contractual o una relación con la Institución deberán conocer y cumplir las normas y disposiciones establecidas en la presente Política de Seguridad de la Información, con el fin de garantizar el adecuado manejo y protección de la información y de la infraestructura tecnológica, asegurando su confidencialidad, integridad y disponibilidad.
- La información personal de las personas involucradas y en general toda la información personal contenida en bases de datos de las cuales la Institución sea responsable, así como los activos de información propios del Politécnico Gran Colombiano, debe ser protegida de acuerdo con lo establecido con la legislación Colombiana vigente, en la Política - Tratamiento y Protección de Datos Personales, Política - Gestión de Datos y conforme al nivel de clasificación y valoración definido por la Institución.
- El incumplimiento de las disposiciones contenidas en la presente Política de Seguridad de la Información dará lugar a la aplicación de las medidas, acciones correctivas, sanciones académicas, disciplinarias, contractuales, administrativas o legales que resulten procedentes, de acuerdo con la naturaleza del vínculo existente entre el infractor y la Institución, así como con la normativa interna y externa aplicable.

Lo anterior aplicará a estudiantes, graduados, colaboradores, docentes, contratistas, proveedores y demás terceros vinculados con el Politécnico Gran Colombiano.

- La Institución implementará procesos continuos para identificar, evaluar, tratar y monitorear riesgos de seguridad de la información y ciberseguridad, alineados con ISO 27001 y NIST.

|                                                           |                             |                                                                       |                                                            |
|-----------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | <b>POLÍTICA</b>             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|                                                           | <b>NOMBRE DEL DOCUMENTO</b> | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

### 4.3 ALCANCE

La presente Política aplica a todos los procesos de la Institución, estudiantes, graduados, colaboradores, profesores de tiempo completo, profesores de catedra, tutores de tiempo completo, tutores de catedra y terceros (proveedores y contratistas), incluidos todos los activos de información que pertenecen o hacen parte de la Institución.

### 4.4 OBJETIVO GENERAL

Establecer los lineamientos, principios, responsabilidades y controles de seguridad de la información y ciberseguridad para proteger la confidencialidad, integridad, disponibilidad y privacidad de la información Institucional, garantizando la protección de los procesos, alineados con los estándares de ISO/IEC 27001 y el marco de ciberseguridad del NIST.

### OBJETIVOS ESPECÍFICOS DE LA POLÍTICA

- Proteger los activos de información institucional frente a amenazas y riesgos internos o externos.
- Establecer criterios para la identificación, clasificación, valoración y protección de los activos de información.
- Fortalecer la confidencialidad, integridad y disponibilidad de la información.
- Establecer lineamientos para la gestión de identidades, accesos y privilegios.
- Promover una adecuada gestión de los riesgos de seguridad de la información y ciberseguridad.
- Establecer lineamientos para la prevención, detección, reporte, gestión y respuesta frente a incidentes de seguridad.
- Fortalecer la seguridad de los servicios tecnológicos, incluyendo servicios en la nube y soluciones contratadas con terceros.
- Establecer responsabilidades de seguridad de la información para colaboradores, estudiantes, contratistas, proveedores y demás usuarios.
- Promover la sensibilización y formación de la comunidad institucional en materia de seguridad de la información y ciberseguridad.
- Establecer mecanismos de seguimiento, evaluación, auditoría y mejora continua del Sistema de Gestión de Seguridad de la Información.

## 5. GRUPOS DE INTERÉS

La presente Política impacta, según su relación con la Institución y el nivel de acceso a la información o a los activos institucionales, a los siguientes grupos de interés:

- Estudiantes.
- Graduados.
- Docentes y tutores.
- Colaboradores.
- Órganos de gobierno y directivos.
- Contratistas.
- Proveedores de bienes y servicios.
- Aliados estratégicos.
- Terceros autorizados.
- Entidades de vigilancia, inspección, control o autoridades competentes, cuando corresponda.

|                                                           |                             |                                                                       |                                                            |
|-----------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | <b>POLÍTICA</b>             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|                                                           | <b>NOMBRE DEL DOCUMENTO</b> | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

## 6. IMPLEMENTACIÓN, SEGUIMIENTO Y EVALUACIÓN

### 6.1 IMPLEMENTACIÓN

La implementación de la presente Política comprende los lineamientos, controles y responsabilidades que se desarrollan a continuación.

#### RESPONSABILIDADES

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Institución, cualquiera que sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

Las directivas institucionales aprueban esta Política y son responsables de la autorización de sus modificaciones.

- La Dirección de Gobierno Digital será responsable de promover, divulgar, coordinar y supervisar el cumplimiento de la presente Política de Seguridad de la Información, así como de definir los lineamientos, estándares y controles requeridos para su adecuada implementación y mejora continua.
- Los propietarios de activos de información: tienen la responsabilidad de mantener integro, confidencial y disponible el activo, mientras sea desarrollado, producido, mantenido, y utilizado.

#### SEGURIDAD DE LOS RECURSOS HUMANOS.

- Ante cambios de cargo o terminación de contrato laboral, el empleado debe hacer entrega formal de los activos de información que le fueron asignados por la Institución para sus actividades laborales, tales como información física, impresa y lógica que se encuentre en medios de almacenamiento externos como discos duros, equipos de cómputo, servidores, bases de datos, entre otros. El jefe de Área son los responsables de recibir dichos activos.
- Las funciones y responsabilidades en materia de Seguridad de la información deben estar incorporadas en la descripción del cargo que desempeña cada empleado.
- Es una obligación de los colaboradores y contratistas aplicar sin excepción la presente política de Seguridad de la Información, así como: conocer, respetar y hacer cumplir las políticas, procedimientos y lineamientos de seguridad definidos y acatar las leyes, decretos y regulación establecida por entes de control.

Para esto EL POLITECNICO GRANCOLOMBIANO debe realizar:

- En la vinculación de personal independientemente de la modalidad de contratación, se debe suscribir un compromiso de cumplimiento de la presente política.
- La Dirección de Gobierno Digital es responsable de proveer los medios necesarios para establecer planear, desarrollar, ejecutar y mantener programas de sensibilización en seguridad de la información, tomando en consideración los roles y responsabilidades definido.

|                                                           |                             |                                                                       |                                                            |
|-----------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | <b>POLÍTICA</b>             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|                                                           | <b>NOMBRE DEL DOCUMENTO</b> | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- Los términos y condiciones relacionados con la seguridad de la información deberán revisarse y actualizarse periódicamente o cuando se presenten cambios normativos, tecnológicos, operacionales o de riesgos.

### SEGURIDAD DE ACTIVOS DE INFORMACIÓN.

- Toda información debe estar identificada, clasificada y valorada acorde con el Procedimiento - Gestión de Activos de Información, definido por la Institución, el cual debe ser ejecutado con la periodicidad requerida en conjunto con los responsables de los inventarios, los propietarios de los activos de información y el Director de Gobierno Digital, quien se va a encargar de actualizarlo cuando sea necesario.
- Los activos de información de la Institución deben estar salvaguardados según su nivel de criticidad.
- Todo activo de información debe contar con los controles definidos, para dar tratamiento a los riesgos identificados los cuales se encuentran identificados en el Procedimiento - Gestión de Activos de Información. Es responsabilidad del propietario del activo verificar la correcta aplicación de los controles.
- Ningún estudiante, empleado o tercero vinculado al Politécnico Grancolombiano puede divulgar información confidencial de la Institución.
- El tratamiento y manejo que tiene el activo de información en la Institución se define acorde a su clasificación dispuesta en el Procedimiento - Gestión de Activos de Información.
- Los activos de información que deban ser enviados o compartidos deben estar etiquetados para este fin, de acuerdo con su nivel de confidencialidad.
- La información digital clasificada como confidencial, debe guardarse y transmitirse de manera cifrada a través de los medios establecidos por la Gerencia de Tecnología e Innovación Digital.
- Los controles para la custodia de información confidencial del Politécnico Grancolombiano deben estar acordes al nivel de su importancia para la Institución y el cumplimiento de dichos controles es una responsabilidad del propietario del activo de información y los custodios.

### SEGURIDAD EN EL CONTROL DE ACCESO LÓGICO.

- Las cuentas de usuario deben ser asignadas a las personas de acuerdo con el rol desempeñado en la Institución y según las necesidades. Solo se concede acceso a la información específica al personal autorizado.
- Toda transacción y actividad realizada con la cuenta de usuario asignada a los sistemas de información de la Institución, es responsabilidad del propietario de dicha cuenta.
- Las contraseñas o cualquier otro método de autenticación deben mantenerse bajo reserva y ser entregadas de forma personal o a través de un medio que asegure su confidencialidad.
- Las cuentas de usuarios, contraseñas o cualquier otro mecanismo de autenticación a los sistemas de información, deben ser tratadas como información confidencial de la Institución, por lo cual no se deben divulgar, publicar ni compartir con ninguna persona.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- e. Todos los accesos deberán gestionarse bajo el principio de mínimo privilegio y necesidad de conocimiento. Los privilegios elevados deberán revisarse al menos semestralmente.
- f. Las cuentas creadas bajo el dominio POLIGRAN, deben contar con doble factor de autenticación, a excepción de las cuentas de servicio.
- g. Las cuentas creadas para los diferentes sistemas de procesamiento de información deben ser deshabilitadas para los estudiantes por mesa de soluciones del área de Tecnología, cuando se interrumpa las funciones en la Institución, para los empleados y proveedores las cuentas deben ser deshabilitadas una vez finalicen o interrumpan sus funciones.
- h. Los empleados, proveedores y contratistas en ejercicio de las actividades consignadas en el contrato firmado con la Institución, no pueden utilizar usuarios genéricos para ningún tipo de actividad.
- i. Los proveedores que tengan acceso a información crítica de la Institución deberán suscribir los acuerdos de confidencialidad que correspondan, en los cuales se establecerá la obligación de implementar y mantener controles de seguridad adecuados. Asimismo, deberán demostrar el cumplimiento de dichos controles mediante certificaciones, auditorías, evaluaciones de riesgo o evidencias equivalentes definidas por la Institución.
- j. Todas las áreas que manejen usuarios (empleados y terceros) deben informar a Tecnología sobre las novedades de los usuarios para realizar los respectivos cambios en los sistemas.
- k. Los perfiles estándar o aquellos que brinden todos los privilegios y accesos a los diferentes sistemas de información, no deben ser asignados en el ambiente productivo, sobre ningún usuario final o rol; exceptuando casos en los cuales por razones propias de la operación se requiera su uso, por lo cual deben estar aprobados por el responsable del área y monitoreadas por la Gerencia de Tecnología e Innovación Digital.
- l. Las carpetas creadas para almacenar información (file server) de los empleados, deben ser administradas teniendo en cuenta la siguiente información:
  - No se deben otorgar permisos de control total.
  - El acceso a las carpetas debe estar limitado al proceso al cual pertenece el usuario.
  - Los permisos para crear, eliminar, ejecutar, leer y modificar se deben limitar de acuerdo con el cargo desempeñado.
- m. Todas las aplicaciones de la Institución deberán ser autenticadas contra el directorio activo, a excepción de ERP SAP.
- n. El cambio de contraseñas se realizará de acuerdo con el nivel de riesgo, eventos de seguridad identificados o cuando exista sospecha de compromiso de credenciales.
- o. El campo de contraseña debe estar parametrizado con las siguientes opciones:
  - La longitud mínima es de 10 caracteres
  - La vigencia de las contraseñas es de 30 días (debe avisar días de caducidad)
  - Debe tener la opción de cambio de contraseña.
  - La contraseña debe cumplir mínimo 3 de las siguientes 4 características:

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- Una mayúscula
- Una minúscula
- Un carácter especial (+\*/\_ {})
- Un número

- p. Las cuentas de usuarios nunca deben estar marcadas con "Password Never Expires" a excepción de las de servicio.
- q. Se prohíbe almacenar sin cifrar, usuarios y contraseñas de acceso a las aplicaciones de la Institución en cualquier medio físico, magnético o electrónico.
- r. Cada 6 meses se realizará depuración de usuarios y se deshabilitarán las cuentas de estudiantes que no hayan tenido ningún tipo de actividad.
- s. La plataforma virtual, dedicada para los estudiantes; deberá tener mecanismos para detección de suplantación del usuario; los cuales deben salvaguardar la información suministrada, para confirmar que efectivamente es el usuario vinculado con la Institución.

## SEGURIDAD SERVICIO DE LA NUBE.

- a. Los servicios de carácter operativo e institucional del Politécnico Grancolombiano que sean implementados o contratados en servicios de nube pública deberán contar con la autorización previa de la Gerencia de Tecnología e Innovación Digital y cumplir los requisitos institucionales de seguridad de la información, protección de datos personales, gestión de riesgos, continuidad del negocio y cumplimiento normativo, incluyendo la clasificación de la información, el cifrado de los datos, la ubicación y transferencia internacional de datos cuando aplique, la gestión de incidentes, el derecho de auditoría y una estrategia de salida del servicio.
- b. Ningún servicio institucional podrá implementarse en servicios de nube pública, privada o híbrida sin la autorización previa de la Gerencia de Tecnología e Innovación Digital y la validación de los requisitos de seguridad de la información, protección de datos personales, gestión de riesgos y cumplimiento normativo aplicables.
- c. El uso de servicios en la nube implica un modelo de responsabilidad compartida para la protección de la información, en el que tanto el proveedor del servicio como el Politécnico Grancolombiano deben asumir y gestionar las responsabilidades que les correspondan en materia de seguridad de la información. En consecuencia, toda contratación de servicios en la nube deberá establecer de manera clara las obligaciones de las partes, así como los requisitos de confidencialidad, integridad y disponibilidad de la información. Adicionalmente, el acuerdo deberá definir los niveles de servicio, los objetivos de desempeño y los mecanismos de seguimiento y control aplicables.
- d. Para todos los servicios en la nube, la Institución debe revisar los acuerdos de servicios con los proveedores, garantizando la implementación de requisitos de seguridad de la información.
- e. Definir funciones y responsabilidades relacionadas con el uso y gestión de los servicios en nube.
- f. Identificar y gestionar los riesgos de seguridad de la información para servicios en nube.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- g. Implementar controles de seguridad de la información para gestionar los servicios de nube prestados por el proveedor, por ejemplo: Segregación de ambientes y controles de acceso a microservicios disponibles en ambiente productivo.
- h. Cualquier riesgo residual que exceda el apetito de riesgo de la Institución, relacionado con el uso de servicio en la nube debe ser identificado y aceptado por el Comité de Riesgo.
- i. Se debe revisar que, en el contrato con los proveedores de nube, se encuentren estipuladas las responsabilidades de cada una de las partes.
- j. Cuando se requiera la implementación de un cambio en diferentes proveedores de servicios en nube se debe contar con un procedimiento de control de cambios definido al interior de la Institución.

#### GESTIÓN DE INCIDENTES.

- a. Los estudiantes, graduados, docentes, colaboradores y terceros deben informar cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información de acuerdo con el PROCEDIMIENTO GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.
- b. Se debe llevar un registro detallado de los incidentes de Seguridad de la Información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo, y de ser posible, la valoración de los daños.
- c. La Institución deberá implementar y mantener herramientas tecnológicas y mecanismos de monitoreo que apoyen la identificación, gestión, seguimiento y respuesta a los incidentes de seguridad de la información.
- d. Los resultados de las investigaciones que involucren a colaboradores, contratistas o terceros deberán ser comunicados a las dependencias competentes, tales como la Gerencia de Talento Humano y Comunicación, la Oficina Jurídica o las autoridades correspondientes, según la naturaleza del incidente.
- e. La Gerencia de tecnología e Innovación Digital debe establecer los mecanismos de control necesarios para recolectar y preservar la evidencia de las investigaciones que se realicen durante el análisis de un incidente de Seguridad de la Información.

#### MANEJO DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

- a. La Dirección de Gobierno Digital debe determinar si el evento reportado corresponde con un incidente de seguridad de la información de acuerdo con los criterios establecidos por el POLITÉCNICO GRANCOLOMBIANO relacionados en el PROCEDIMIENTO GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.
- b. El POLITÉCNICO GRANCOLOMBIANO debe desarrollar actividades para la recolección de evidencia durante la gestión del incidente, la cual podrá ser utilizada cuando se requieran acciones disciplinarias o acciones legales, en cuyo caso se contratará un experto forense. La evidencia recolectada no debe ser manipulada y debe cumplir con los requisitos legales correspondientes.
- c. Se debe documentar para cada uno de los incidentes presentados las lecciones aprendidas, con el fin de contar con una base completa de conocimiento que le permita analizar, recopilar, cuantificar y monitorear la información, así como establecer las actividades para resolver incidentes similares en el futuro. Del mismo modo

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

la base de lecciones aprendidas permitirá capacitar al personal involucrado con ejemplos claros de lo que puede suceder, como responder a los incidentes y que acciones se debe implementar para evitar su materialización en el futuro.

### CORREO ELECTRÓNICO.

- a. El acceso al correo electrónico está reservado para todos aquellos estudiantes, graduados y empleados que lo requieran de acuerdo con las necesidades y desempeño de las funciones propias.
- b. Las cuentas de usuario asignadas a contratistas y demás terceros deberán crearse con una fecha de expiración definida, acorde con la vigencia de la relación contractual o la necesidad del servicio. Una vez cumplido el plazo establecido o finalizada la vinculación, los accesos deberán ser deshabilitados o eliminados de manera oportuna, de acuerdo con los procedimientos definidos por la Institución.
- c. Los mensajes por correo electrónico son considerados parte de los registros de los activos de información, por lo que están sujetos a políticas de monitoreo, auditoría e investigación de eventos.
- d. No se permite utilizar el correo electrónico institucional para actividades personales o comerciales no autorizadas, mensajes en cadena, juegos, publicidad no corporativa, contenidos discriminatorios, racistas, sexistas, pornográficos, difamatorios, amenazantes, maliciosos o cualquier otro contenido ajeno a las finalidades institucionales que vulnere derechos de terceros o comprometa la seguridad de los activos de información. Las restricciones previstas en este literal no podrán interpretarse o aplicarse de manera que desconozcan las libertades religiosas, políticas, sindicales o de expresión protegidas por la Constitución y la ley, siempre que su ejercicio resulte compatible con las actividades propias del cargo y con las reglas institucionales aplicables.
- e. La transmisión de mensajes en forma masiva en la Institución utilizando el correo electrónico (más de 500 correos al día), es realizado única y exclusivamente por la Dirección de Comunicaciones.
- f. Las cuentas de servicio o cuentas genéricas autorizadas por la Institución, tales como las utilizadas para Huella Grancolombiana, Movilidad, Prácticas Empresariales, Responsabilidad Social y otros procesos institucionales, podrán ser empleadas para el envío de comunicaciones y comunicados institucionales. El uso de estas cuentas deberá realizarse en cumplimiento de las políticas institucionales y de las disposiciones aplicables en materia de protección y tratamiento de datos personales.
- g. Las cuentas de servicio utilizadas por los Centros de Servicio Universitario (CSU) están autorizadas para establecer comunicaciones personalizadas con los usuarios en el desarrollo de sus funciones institucionales. El uso de estas cuentas deberá realizarse de conformidad con los lineamientos institucionales y las disposiciones aplicables en materia de protección y tratamiento de datos personales.
- h. Todas las comunicaciones emitidas y/o recibidas por correo electrónico, deben preservar la conducta ética y profesional que el remitente y/o destinatario debe mantener como miembro de la Institución.
- i. La capacidad otorgada para los usuarios en licenciamiento de servicios MICROSOFT es, estudiante 500 megas (0.5 GB) y colaboradores 30 GB.
- j. El correo electrónico corporativo asignado a cada colaborador es de uso estrictamente personal e intransferible. Su utilización está reservada exclusivamente para el titular de la cuenta, quien es responsable de todas las actividades realizadas a través de ella. En consecuencia, se prohíbe compartir, ceder, prestar o permitir el acceso

|                                                           |                             |                                                                       |                                                            |
|-----------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | <b>POLÍTICA</b>             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|                                                           | <b>NOMBRE DEL DOCUMENTO</b> | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

a terceros, ya sean internos o externos a la organización, con el fin de garantizar la seguridad de la información, la confidencialidad de las comunicaciones y la adecuada gestión de los recursos tecnológicos de la entidad.

- k. Si se reciben mensajes con archivos adjuntos o enlaces de dudosa procedencia, no se deben abrir ya que pueden contener software malicioso como virus y troyanos que afecten los sistemas de información de la Institución. Estos casos se deben reportar a la Mesa de Soluciones y manejarlo como un incidente a la Gerencia de Tecnología e Innovación Digital.

## REVISIÓN DE CUENTAS DE CORREO ELECTRÓNICO.

Para efectos de la presente política, la revisión de cuentas de correo electrónico corresponde a las actividades de monitoreo, auditoría, verificación de cumplimiento de controles de seguridad, análisis de eventos e investigación de incidentes de seguridad de la información que la Institución podrá realizar sobre las cuentas de correo corporativo. Estas actividades deberán efectuarse de conformidad con la legislación aplicable, los principios de necesidad, proporcionalidad, confidencialidad, debido proceso y respeto por los derechos de los titulares de la información.

- a. Revisar y monitorear el cumplimiento de las Políticas de Seguridad establecidas para el uso del servicio de correo electrónico, generando las acciones necesarias para prevenir posibles eventos o incidentes de seguridad. Así mismo, contar con la facultad de revisar los buzones de correo electrónicos corporativos de personal comprometido por incidentes de seguridad, siguiendo técnicas forenses y cadenas de custodia.
- b. Para la verificación en los equipos de cómputo, se pueden usar procedimientos de auditoría manual, técnica de auditoría forense con ayuda de computadores o herramientas especializadas, o una combinación de ambos para obtener suficiente material de evidencia.
- c. Desde la Dirección de Gobierno Digital se deberá realizar monitoreos de manera periódica y validar el uso del correo electrónico corporativo para dar de baja aquellas cuentas que no sean utilizadas. Adicionalmente, se deberá realizar una depuración semestral.
- d. El uso del correo electrónico corporativo es un servicio del Politécnico Grancolombiano, que puede ser revocado en cualquier momento si se detecta una conducta abusiva. Cualquier violación a las políticas corporativas de seguridad de la información puede acarrear una suspensión temporal o permanente de la cuenta de correo electrónico, sin perjuicio de las acciones que pueda iniciar la Institución.
- e. La Dirección de Gobierno Digital, se reserva el derecho de retirar el servicio con previo aviso, ante violaciones de la Política de ética y Buen Gobierno, reglamento o políticas institucionales de seguridad de la información.
- f. Toda solicitud de revisión, monitoreo especial o investigación sobre cuentas de correo corporativo deberá estar debidamente justificada, documentada y avalada por la Dirección Jurídica, observando los principios de necesidad, proporcionalidad, finalidad y debido proceso.
- g. Se le deberá informar al Director de Gobierno Digital cualquier tipo de incidente con respecto a la violación o mal uso del correo corporativo del Politécnico Grancolombiano, el cual aprobará la suspensión del servicio hasta tanto no se cuente con el informe del análisis realizado por la Institución y las acciones realizadas no se restablecerá el servicio para dicho usuario.
- h. El Director de Gobierno Digital es el encargado de investigar los incidentes de seguridad relacionados con las cuentas de correo electrónico. Para ello cuenta con la colaboración de Tecnología para la entrega de información que sea requerida durante la investigación. Además, es el encargado de informar a la Gerencia de

|                                                           |                             |                                                                       |                                                            |
|-----------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | <b>POLÍTICA</b>             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|                                                           | <b>NOMBRE DEL DOCUMENTO</b> | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

Tecnología e Innovación Digital sobre los resultados de su investigación para su posterior notificación a Gestión de Talento Humano.

- i. Cuando se considere necesario, el Director de Gobierno Digital podrá coordinar con las áreas técnicas y/o especializadas la recopilación y análisis de las evidencias disponibles, con el propósito de aportar elementos que permitan establecer las circunstancias asociadas al posible uso inadecuado de los activos de información.

### USO DE INTERNET.

- a. Los usuarios del servicio de internet de la Institución deben hacer uso eficiente del mismo en relación con las actividades de su desempeño.
- b. Los usuarios del servicio de internet deben evitar la descarga de software, así como su instalación en las estaciones de trabajo de la Institución.
- c. No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, hacking y/o cualquier otra página que vaya en contra de la ética, la moral, las leyes vigentes o políticas establecidas en este documento.
- d. No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.
- e. La única plataforma de almacenamiento (respaldo) autorizada por la Institución es: Microsoft OneDrive (nube) y los file servers (almacenamiento local). Adicionalmente, se garantiza el respaldo del correo en la nube con una retención de 30 días calendario. Cualquier otro tipo de almacenamiento en red o nube debe ser autorizado por el Comité de Estrategia Digital y Gobierno de Datos.
- f. Todos los colaboradores tendrán internet, para ejercer sus labores asignadas; si por algún motivo de acuerdo con sus funciones necesita acceder a otras páginas de consulta debe hacer la solicitud a Tecnología, para que se le asigne el acceso a internet avanzado.
- g. El acceso a Internet está reservado para todos aquellos empleados, estudiantes, docentes de catedra y terceros que lo requieran según sus funciones.
- h. La Institución restringe el acceso a sitios de internet que por alguna circunstancia vayan en contra de sus políticas institucionales, políticas de seguridad y buenas prácticas adoptadas por la institución, tales como consultar material ilegal, de acoso, difamatorio, abusivo, amenazador, nocivo, vulgar, obsceno o de cualquier otra manera censurable.
- i. Está prohibido para los empleados y terceros el acceso a red inalámbrica o cableada del Politécnico Gran Colombiano, menoscabar o eludir los controles establecidos por la Institución para la protección de los activos de información.
- j. Cualquier tipo de ataque, así como efectuar un escaneo, prueba o penetración de sistemas de computación, redes en Internet, o redes internas, está estrictamente prohibido, salvo en casos debidamente autorizados por la Gerencia de Tecnología e Innovación Digital y por requisitos propios de la Institución.
- k. Los sistemas de comunicación tales como modems, routers, switch, entre otros dispuestos por el Politécnico Gran Colombiano, son los únicos autorizados para su uso en la red de la Institución.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b><br><i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|---------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b><br><i>Registrado por secretaría general</i>  | <b>Versión:</b><br><i>Registrado por el sistema integrado</i> |

- I. Queda prohibido toda publicación o intercambio de información sensible de la Institución a través de cualquier medio físico, magnético o electrónico sin el consentimiento y la respectiva autorización del responsable de su manejo y en cumplimiento de los controles establecidos para la protección de la información.

## INSTALACIÓN Y USO DE PCS, PERIFÉRICOS Y MEDIOS DE ALMACENAMIENTO EXTRAÍBLES.

- a. En caso de usar algún medio de almacenamiento extraíble, éste debe ser verificado previamente por el software antivirus proporcionado por la Gerencia de Tecnología e Innovación Digital. Las únicas áreas para utilizar discos externos de gran capacidad son Centro de Medios, Departamento de Comunicaciones y Agencia Trompo.
- b. Con el fin de proteger la información y el acceso a la red de la Institución, los empleados deben dejar su equipo portátil asignado en un lugar seguro o con la guaya suministrada por la Gerencia de Tecnología e Innovación Digital.
- c. No está autorizado el uso de recursos informáticos (datos, hardware, software, redes, servicios) y de telecomunicaciones (teléfono) para actividades que no estén autorizadas o relacionadas con el objeto social de la Institución o diferentes a las funciones asignadas al cargo que desempeña el empleado.
- d. Ningún usuario es administrador de los equipos de cómputo asignados por la Institución. Solo se realizará la excepción en caso de que por sus labores dentro de la Institución deba tener este privilegio, el cual debe ser autorizado por medio de una carta de aceptación de riesgos en donde se detalla el impacto, los controles a implementar y la responsabilidad que tiene sobre el mismo.
- e. Ninguna aplicación, sistema, dispositivo de hardware, computadores o en general cualquier recurso que tenga que ver con Tecnologías de Información puede ser utilizado en el ambiente tecnológico de la Institución sin contar con los controles mínimos o estándares de seguridad establecidos y sin previa autorización de la Gerencia de Tecnología e Innovación Digital
- f. Todos los equipos de cómputo de uso personal pertenecientes a la Institución deben contar con password en el BIOS, en donde el único custodio de esta información sea el personal de Soporte Nivel I.
- g. No está permitido el almacenamiento de información personal sin derechos de autor en la red o file servers de la Institución.

## DISPOSITIVOS MÓVILES.

- a. Todo dispositivo móvil (tablets, teléfonos inteligentes, entre otros) con acceso a la red y de propiedad de la Institución, deben sin excepción, ser configurados con los controles mínimos definidos en los estándares de seguridad para dispositivos móviles.
- b. Está prohibido el uso de funciones de equipos móviles como medio de almacenamiento, grabación y captura de información confidencial de la Institución a la que el usuario no esté autorizado.
- c. En caso de pérdida o hurto de un dispositivo móvil que se encuentre autorizado para acceder a las aplicaciones o información de la Institución, el colaborador debe realizar las actividades definidas en el Procedimiento - Retiro de Activos Fijos y adicional reportar la novedad a Mesa de Soluciones, además de realizar el cambio de clave con

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

la cual ingresa a las diferentes aplicaciones, a través de las distintas formas que ofrece la Institución, para así evitar accesos no autorizados a la información.

### ESCRITORIO LIMPIO.

- En horas no hábiles, o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deben dejar los medios que contengan información crítica, protegida bajo llave.
- Los usuarios deben bloquear su estación cada vez que se retiren de su puesto de trabajo y solo se podrá desbloquear con la contraseña del mismo usuario que la bloqueó.
- Todas las estaciones de trabajo deben usar únicamente el papel tapiz y el protector de pantalla establecido por el Institución.
- Los usuarios no deberán almacenar en el escritorio de sus estaciones de trabajo información institucional clasificada, documentos sensibles, ni accesos directos a sistemas de información críticos. La información deberá almacenarse únicamente en los repositorios institucionales autorizados, de acuerdo con su clasificación y los lineamientos de seguridad establecidos.
- Los usuarios son responsables por la custodia y el uso adecuado de los activos informáticos que les sean asignados. Durante la ejecución de actividades de mantenimiento, actualización o soporte técnico sobre dichos activos, deberán estar presentes o garantizar su entrega formal al personal autorizado, con el fin de preservar la seguridad de la información y mantener la cadena de custodia del equipo.

### TELETRABAJO Y TRABAJO EN CASA.

- Los usuarios que por razones propias de la Institución se encuentren autorizados para realizar teletrabajo o trabajo en casa, son responsables por la protección física del equipo asignado contra acceso, uso no autorizado, hurto, pérdida o daño de información confidencial institucional.
- Las conexiones que se realicen desde y hacia los equipos destinados para teletrabajo, se deben hacer a través de ZTNA con el fin de dar aseguramiento a los activos de información de la Institución.
- La Gerencia de Tecnología e Innovación Digital implementa los controles necesarios para el aseguramiento de los equipos de teletrabajo contra acceso lógico no autorizado, protección de la información y la red de la Institución.
- Cuando las reuniones, clases, capacitaciones o actividades virtuales requieran ser grabadas, deberá informarse previamente a los participantes y cumplirse las disposiciones institucionales aplicables en materia de protección de datos personales y tratamiento de la información.
- Todos los usuarios deberán cumplir con las políticas de seguridad de la información que se implementan dentro de los recursos tecnológicos para el cumplimiento de sus labores; por ningún motivo debe ser alterada dichas configuraciones.
- Los elementos tecnológicos suministrados no podrán ser usados por persona distinta al teletrabajador, quien a la terminación del contrato deberá restituir los objetos entregados, en buen estado, salvo el deterioro natural;

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b><br><i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|---------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b><br><i>Registrado por secretaría general</i>  | <b>Versión:</b><br><i>Registrado por el sistema integrado</i> |

cuya verificación será realizada por el COMITÉ DE ACTIVOS FIJOS quienes deciden que acción se deben tomar.

- g. El acceso a los diferentes entornos y sistemas de información de la Institución será efectuado siempre y en todo momento bajo el control y la responsabilidad del Teletrabajador; siguiendo los procedimientos establecidos por la Gerencia de Tecnología e Innovación Digital.
- h. El Teletrabajador se compromete a respetar la legislación en materia de protección de datos, las políticas de privacidad y de seguridad de la información que la Institución ha implementado, como también a:
- i. Utilizar los datos de carácter personal y confidencial a los que tenga acceso único y exclusivamente para cumplir con sus obligaciones para con la Institución.
- j. Cumplir con las medidas de seguridad que la Institución haya implementado para asegurar la confidencialidad, secreto e integridad de los datos de carácter personal y confidencial a los que tenga acceso, así como no ceder en ningún caso a terceras personas esta información, ni tan siquiera a efectos de su conservación; salvo que para tal fin cuente con autorización del titular.

## ARTÍCULO 20: SISTEMAS DE INFORMACIÓN.

- a. La Dirección de Comunicaciones Internas, es la única autorizada para administrar la información que se publica en canales de comunicación. Los departamentos que realizan publicaciones de investigación solamente están autorizados para hacerlo en plataformas educativas.
- b. La Dirección de Comunicaciones Internas es la única dependencia autorizada para publicar información institucional, crear usuarios en redes sociales, blogs, utilizar logos o divulgar cualquier otro tipo de contenido en nombre de la Institución. No obstante, los órganos de participación reconocidos por la Institución podrán administrar sus propias redes sociales y canales de comunicación, así como utilizar los logos institucionales previamente autorizados y publicar información relacionada con sus actividades y con asuntos que involucren al Politécnico Gran Colombiano, siempre que dichas publicaciones se realicen en cumplimiento de los lineamientos institucionales de comunicación, imagen corporativa, seguridad de la información y protección de datos personales.
- c. Toda instalación, configuración, mantenimiento y actualización de hardware y software debe ser realizada por la Gerencia de Tecnología e Innovación Digital a excepción de las personas que cuentan con autorización por parte del responsable del área.
- d. La Institución se reserva el derecho de administrar el almacenamiento de los servicios de almacenamiento que se administren. En consecuencia, la Gerencia de Tecnología E Innovación Digital podrá eliminar, depurar o disponer de la información almacenada en dichos recursos cuando sea necesario para garantizar la capacidad, disponibilidad, continuidad de los servicios tecnológicos o el cumplimiento de las políticas institucionales de retención y gestión de la información. Es responsabilidad de los usuarios conservar la información crítica en los repositorios institucionales autorizados y cumplir con las directrices de clasificación, conservación y disposición de la información.

## SEGURIDAD DE ACTIVOS DE INFORMACIÓN.

- a. Toda información debe estar identificada, clasificada y valorada acorde con el procedimiento TI-PR-001

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

Gestión de Activos de Información definido por la Institución, el cual debe ser ejecutado con la periodicidad requerida en conjunto con los responsables de los inventarios, los propietarios de los activos de información y el Director de Gobierno Digital, quien se va a encargar de actualizarlo cuando sea necesario.

- b. Los activos de información de la Institución deben ser salvaguardados por cada líder de proceso o persona encargada de la custodia del activo de información; en las diferentes plataformas tecnológicas suministradas por las Institución.
- c. Todo activo de información debe contar con los controles definidos, para dar tratamiento a los riesgos identificados los cuales se encuentran determinados en el procedimiento TI-PR-001 Gestión de Activos de Información. Es responsabilidad del propietario del activo de información verificar la correcta aplicación de los controles.
- d. Ninguna persona vinculada al Politécnico Grancolombiano sea, estudiante, colaborador o tercero puede divulgar información confidencial de la Institución.
- e. El tratamiento y manejo que tiene el activo de información en la Institución se define acorde a su clasificación dispuesta en el procedimiento TI-PR-001 Gestión de Activos de Información.
- f. Los activos de información que deban ser enviados o compartidos deben estar etiquetados o rotulados para este fin, de acuerdo con su nivel de confidencialidad.
- g. La información digital clasificada como confidencial, debe guardarse y transmitirse de manera cifrada a través de los medios establecidos por la Gerencia de Tecnología e Innovación Digital.
- h. Los controles para la custodia de información confidencial del Politécnico Grancolombiano deben estar acordes al nivel de su importancia para la Institución y el cumplimiento de dichos controles; esto es una responsabilidad del propietario del activo de información y los custodios.

## CLASIFICACIÓN DE LA INFORMACIÓN

- a. Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere la Institución como, por ejemplo:
  - Formularios
  - Comprobantes propios o de terceros.
  - Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
  - Otros soportes magnéticos/electrónicos removibles, móviles o fijos. o Información transmitida vía oral o por cualquier otro medio de comunicación.
- b. El Politécnico Grancolombiano estableció en el procedimiento TI-PR-001 Gestión de Activos de Información los criterios para realizar la valoración de los mismos respecto a su nivel de confidencialidad, integridad y disponibilidad.
- c. De acuerdo con la clasificación otorgada al activo establecerá los niveles de acceso, restricciones o permisos autorizados a los documentos físicos y digitales, sistemas de información y/o cualquier aplicativo

|                                                           |                             |                                                                       |                                                            |
|-----------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | <b>POLÍTICA</b>             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|                                                           | <b>NOMBRE DEL DOCUMENTO</b> | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

que contenga el activo de información con el fin de preservar su confidencialidad, integridad y disponibilidad.

- d. Toda la información debe ser identificada, clasificada y documentada. Los usuarios responsables de la información del Politécnico Grancolombiano, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

## ETIQUETADO DE LA INFORMACIÓN

Independientemente de su formato, medio o ubicación, la información se clasificará como INFORMACIÓN PÚBLICA RESERVADA, INFORMACIÓN PÚBLICA CLASIFICADA (PRIVADA Y SEMI-PRIVADA) e INFORMACIÓN PÚBLICA siguiendo el esquema de clasificación de la información adoptada por Politécnico Grancolombiano y documentada en el procedimiento TI-PR-001 Gestión de Activos de Información.

## TRANSFERENCIA DE INFORMACIÓN

- a. Se debe evitar la divulgación, modificación o eliminación no autorizada de los activos de información que lleguen a afectar cualquiera de las operaciones de Politécnico Grancolombiano.
- b. Se debe contar con controles de transferencia formales para proteger el intercambio de información, independientemente del medio de comunicación utilizado; del mismo modo se debe implementar controles para prevenir el acceso no autorizado, la copia, modificación, enrutamiento incorrecto, destrucción y denegación de servicio.
- c. Se debe establecer acuerdos con terceros para la transferencia segura de información entre el Politécnico Grancolombiano y las partes externas a la Institución (proveedores, aliados y demás terceros).
- d. Se debe proteger la información incluida en los mensajes electrónicos de acuerdo con el nivel de clasificación que contenga.
- e. Los propietarios de la información que se requiera transferir son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de esta; por su parte, los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad y disponibilidad de acuerdo con la documentación vigente. o Los acuerdos de transferencia deben en todo caso velar por el cumplimiento de las regulaciones legales, propiedad intelectual y protección de datos personales. Así mismo deben especificar las consideraciones de seguridad y reserva de la información, y las responsabilidades por el mal uso o divulgación de esta.

## CUMPLIMIENTO REGULATORIO.

- a. La Institución vela por el cumplimiento de la presente política y de la Legislación aplicable vigente por los entes de control.
- b. La Gerencia de Tecnología e Innovación Digital en conjunto con la Secretaría General, definen e implementan los controles necesarios para dar cumplimiento y protección a los activos de información.

|                                                    |                             |                                                                |                                                     |
|----------------------------------------------------|-----------------------------|----------------------------------------------------------------|-----------------------------------------------------|
| <b>PROCESO:</b><br>Mencionar el nombre del proceso | <b>POLÍTICA</b>             | <b>Acuerdo - Resolución:</b> Registrado por secretaría general | <b>Código:</b> Registrado por el sistema integrado  |
|                                                    | <b>NOMBRE DEL DOCUMENTO</b> | <b>Fecha aprobación:</b> Registrado por secretaría general     | <b>Versión:</b> Registrado por el sistema integrado |

## SEGURIDAD FÍSICA.

- a. Todo espacio físico en el cual se ubique infraestructura tecnológica necesaria para la operación de la Institución debe contar con controles de acceso para la restricción de personal no autorizado, tales como los centros de cómputo, centros de cableado, entre otros.
- b. Deben existir controles ambientales operando eficientemente en las sedes en las cuales se encuentre la infraestructura tecnológica necesaria para la operación de la Institución, tales como centros de cómputo, centros de cableado, entre otros.
- c. Todo ingreso de personas a los centros de cómputo de la Institución debe quedar registrado en el Formato - Bitácora de ingreso de visitantes.
- d. El acceso físico a los centros de procesamiento de datos y cableado de todas las sedes es responsabilidad de la Gerencia de Tecnología e Innovación Digital.
- e. Toda persona que visite las instalaciones de las diferentes sedes del Politécnico Grancolombiano debe cumplir con los controles de acceso físico dispuestos por la Institución.
- f. El movimiento o traslado de equipos de cómputo, recursos informáticos y de comunicaciones, debe realizarse únicamente en coordinación con el área de Activos Fijos con el fin de evitar pérdida, hurto o daño de los activos de información de la Institución.
- g. La información física sensible de la Institución debe guardarse bajo llave (gabinete, archivador u otro medio físico seguro) cuando no está en uso, especialmente ante ausencias temporales o prolongadas y según el riesgo catalogado para el activo de información.
- h. Cualquier alteración en la información que se haga por medio de los equipos de la Institución, por descuido del usuario, es de su responsabilidad. Se aplicará el bloqueo de sesión después de 5 minutos de inactividad, para evitar que el computador quede expuesto y se use de manera no autorizada, a excepción de los equipos que están ubicados en los salones de clase.
- i. Para el caso de activos fijos propiedad de la Institución que se encuentren extraviados, el Jefe Administrativo o el Coordinador de Servicios Administrativos debe entregar a Activos Fijos el elemento encontrado, relacionándolo en una planilla simple remitida por correo electrónico.
- j. Los equipos tecnológicos se almacenan en bodegas destinadas para tal efecto, bajo la responsabilidad de la Gerencia de Tecnología e Innovación Digital.
- k. El personal vinculado a la Institución solo debe tener acceso única y exclusivamente a los espacios de la Institución de acuerdo con su rol y función.
- l. Los componentes, equipos de procesamiento de información, comunicaciones y archivos importantes para la Institución, deben estar ubicados en espacios de acceso restringido a personal no autorizado, empleando mecanismos de control como tarjetas de proximidad, esquemas biométricos, cerraduras, entre otros. Así mismo, deben contar con cámaras de video que permitan grabar el flujo de personas que entran y salen de dichos espacios.
- m. Es responsabilidad de cada uno de los procesos, notificar al Coordinador de Servicios Administrativos la ubicación de dichos elementos y asignar el presupuesto suficiente para establecer los controles necesarios.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b><br><i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|---------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b><br><i>Registrado por secretaría general</i>  | <b>Versión:</b><br><i>Registrado por el sistema integrado</i> |

- n. Es responsabilidad de cada uno de los procesos establecer los controles físicos necesarios que establezca la Coordinador de Servicios Administrativos dentro de su análisis de riesgos.
- o. Los computadores y fotocopadoras de los edificios, oficinas administrativas y demás sedes de la Institución deben estar inventariados por el software de control de impresiones para evitar el uso no autorizado.

### SEGURIDAD DE LAS OPERACIONES - BACKUPS DE LA INFORMACIÓN.

- a. Toda la información CLAVE Y SENSIBLE que se encuentra almacenada en las plataformas tecnológicas de la Institución, debe contar con actividades periódicas de backups, el cual es realizado por el personal de Operaciones IT para garantizar acciones de restauración confiables en casos de emergencia y según sea requerido y autorizado por el responsable del activo de la información.
- b. El respaldo de las bases de datos del Politécnico Grancolombiano relacionado con las aplicaciones críticas se realiza diariamente. Estas copias son destinadas únicamente para dar continuidad a los procesos que se ejecutan en la Institución.

### INSTALACIÓN Y USO DE SOFTWARE.

- a. Todas las adquisiciones de software deben estar avaladas por la Gerencia de Tecnología e Innovación Digital y por el responsable del área.
- b. No se permite descargar, instalar o ejecutar software sin la debida revisión y autorización de la Gerencia de Tecnología e Innovación Digital a excepción de las personas que por sus actividades cuentan con la autorización correspondiente.
- c. Todo el software adquirido por la Institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está prohibido hacer copias o usar este software para fines personales o comerciales

### SEGURIDAD DE REDES.

- a. Todos los equipos de comunicaciones deben estar protegidos físicamente contra robo y manipulación de personal no autorizado, por lo que siempre deben estar instalados en centros de datos o gabinetes destinados para este fin.
- b. El área infraestructura tecnológica debe poseer un inventario detallado de todos los dispositivos de comunicaciones en donde se debe especificar al menos su nombre en la red, modelo, versión de software, ubicación física, estado del soporte y última actualización.
- c. La Institución deberá ejecutar análisis periódicos de vulnerabilidades sobre infraestructura crítica, aplicaciones, servicios en nube y activos tecnológicos, documentando su tratamiento.
- d. El único personal autorizado para manipular y configurar los equipos de red es el área de Operaciones IT del Politécnico Grancolombiano. Si por alguna razón, alguien diferente dentro o fuera de la institución debe manipular o configurar equipos, este personal debe ser debidamente autorizado por la Dirección de Operaciones IT.
- e. Todo dispositivo de comunicaciones considerado como crítico, debe tener redundancia lógica y física. Las excepciones deben documentarse.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b><br><i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|---------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b><br><i>Registrado por secretaría general</i>  | <b>Versión:</b><br><i>Registrado por el sistema integrado</i> |

- f. Las redes de datos deben estar aisladas y divididas en zonas, según las necesidades de la Universidad. Debe existir al menos una zona privada y una zona protegida (DMZ) que aisle los servicios que serán publicados hacia redes externas. Es responsabilidad del área de Operaciones IT, diseñar la red bajo el principio de acceso mínimo.
- g. Cuando se realicen conexiones con terceros, se deben asegurar que los terceros únicamente tengan acceso a los equipos y servicios estrictamente necesarios (principio de mínimo acceso).
- h. La red desde donde se gestionan los equipos de comunicaciones, debe ser una red únicamente destinada con este fin. En todos los casos posibles debe restringirse el acceso a la administración de equipos desde otras redes.
- i. Deben existir al menos dos servidores DNS diferentes: uno para la solicitud interna y otro para las solicitudes externas (usuarios de internet). 10. Todos los equipos de comunicaciones deben ser monitoreados y deben tener logs activos. Los logs de monitoreo deben almacenarse por 6 meses mínimo. Cualquier excepción debe ser autorizada por las direcciones de Operaciones IT y Gobierno Digital.
- j. Las contraseñas de administración de los equipos de comunicaciones deben componerse de mayúsculas, minúsculas, números y caracteres especiales. Deben ser mínimo de 10 caracteres; estas deben estar protegidas con PAM.
- k. No mostrar el último usuario que accedió exitosamente al sistema, ni ningún historial de nombres de usuario.
- l. Todos los equipos de comunicaciones deben cumplir con las configuraciones y guías del proveedor relacionadas con las buenas prácticas de seguridad. Es responsabilidad del área de infraestructura tecnológica y terceros, implementar dichas configuraciones y aplicarlas en toda nueva instalación y configuración. El Director de Gobierno Digital definirá estándares de configuración segura para los equipos que se considere necesario, los cuales serán de obligatorio cumplimiento.
- m. Todas las configuraciones, esquemas, topologías y demás información de la red deben ser documentada y almacenada en un repositorio seguro con acceso restringido.
- n. El área de Operaciones IT debe documentar los procedimientos de operación.
- o. Se deben instalar periódicamente parches de seguridad y actualizaciones para el software de todos los equipos de comunicaciones. Es responsabilidad del área de infraestructura tecnológica, realizar todas las pruebas pertinentes antes de realizar actualizaciones en ambientes productivos. Se debe llevar un registro de todos los parches y actualizaciones aplicados, o su debida justificación en caso de no aplicarlos.
- p. El área de Operaciones IT debe realizar backup mensual de los equipos de red y almacenarlos en un lugar diferente al mismo equipo respaldado; deben almacenarse en un repositorio seguro y de acceso restringido. Antes y después de cualquier modificación sobre los equipos de comunicaciones debe realizarse backup.
- q. Los administradores de los equipos de comunicaciones deben asegurar que ningún dispositivo de red tenga la contraseña por defecto. Para los equipos en los cuales sea posible, también debe renombrarse el usuario.
- r. Los nombres de los equipos, usuarios y contraseñas de acceso no deben permitir la identificación de la importancia o criticidad de los equipos (ej.: usuarios o contraseñas de acceso con la palabra admin).

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | <b>POLÍTICA</b>             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | <b>NOMBRE DEL DOCUMENTO</b> | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- s. El área de Operaciones IT debe establecer controles para evitar que el personal no autorizado tenga conexión a las redes de datos del Politécnico Grancolombiano.
- t. El área de Operaciones IT es responsable de realizar la gestión de accesos a los administradores de los equipos de comunicaciones, siguiendo los lineamientos del Procedimiento - Gestión de Accesos.
- u. Todos los protocolos de gestión de red deben estar protegidos con password y deben seguir las buenas prácticas de seguridad.
- v. No se deben utilizar protocolos obsoletos o que representen un riesgo para la Seguridad de la Información. Cualquier excepción debe ser evaluada y autorizada por la Gerencia de Tecnología e Innovación Digital.
- w. El tráfico sensible debe estar cifrado en la red.
- x. Los dispositivos de comunicaciones no deben almacenar contraseñas en texto plano.
- y. El Director de Gobierno Digital realizará pruebas de vulnerabilidades a los equipos de comunicaciones al menos una vez al año. Las vulnerabilidades encontradas deben ser tratadas por el área de infraestructura tecnológica y los involucrados pertinentes según sea el caso. (Ver Procedimiento – Gestión de Vulnerabilidades).
- z. Las conexiones para la gestión y administración de los equipos deben ser cifrada.
- aa. Los administradores de los equipos de comunicaciones deben establecer niveles de servicio adecuados a las necesidades del Politécnico Grancolombiano.
- bb. Las redes inalámbricas deben organizarse según la necesidad de los usuarios. Para las redes críticas con información confidencial debe evitarse propagar el nombre de la WLAN.
- cc. En caso de detectar violaciones a las políticas y procedimientos establecidos, o al realizar un mal uso de la red, se debe restringir el acceso inmediatamente.
- dd. Es responsabilidad del área de Operaciones IT, auditar logs en las redes y detectar accesos no autorizados al menos una vez al mes. Estos accesos no autorizados deben notificarse al Director de Gobierno Digital.
- ee. Está prohibido usar protocolos de cifrado débil para las redes inalámbricas.
- ff. Establecer múltiples rutas a la PSTN, así como líneas análogas de emergencia.
- gg. Todas las conexiones hacia terceros deben aislarse por un firewall diferente al que se utiliza para acceder a internet y a cualquier otra conexión externa.
- hh. Los terceros deben firmar un documento de condiciones para garantizar una conexión segura antes de otorgar acceso.
- ii. El área de Gobierno Digital debe realizar auditorías y definir la responsabilidad para terceros que ingresen y gestionen equipos del Politécnico Grancolombiano. Regularmente se debe realizar auditoria a los proveedores.
- jj. Deben configurarse VLANS para segregar servicios dentro del datacenter para proteger los servicios más sensibles

|                                                           |                             |                                                                       |                                                            |
|-----------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | <b>POLÍTICA</b>             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|                                                           | <b>NOMBRE DEL DOCUMENTO</b> | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

## CONEXIONES REMOTAS.

- Toda conexión remota a la red de la Institución debe realizarse a través de canales seguros como o canales dedicados. Éstas deben solicitar autenticación para establecer la conexión remota a la red con el fin de prevenir accesos no autorizados.
- El uso de la ZTNA es exclusivo de quienes se conectan por medio de WIFI dentro de las instalaciones de la Institución y de los que no se encuentren dentro de la red LAN del Politécnico Gran Colombiano y deban hacer uso de sistemas de información de manera remota debido a las exigencias particulares de sus actividades. Adicionalmente, está permitido el uso de ZTNA a quienes deban correr procesos en horarios no laborales, con previa autorización.
- Toda autorización para conexión remota por parte de proveedores deben tener una vigencia, una contraseña de acceso y una cuenta de usuario que debe ser bloqueada una vez finalizada las labores para las cuales se creó; el empleado responsable del proveedor es quien notifica por medio de la Mesa de Soluciones la vigencia del acceso; cualquier daño, anomalía y novedad que suceda después de la culminación de las labores del proveedor y esta no fuera notificada, la responsabilidad recae sobre el usuario responsable del proveedor.
- Toda conexión remota sea de los empleados o proveedores de la Institución, es monitoreada y puede ser bloqueada en caso de identificar situaciones inusuales respecto al uso de la cuenta y el acceso a los activos de información.
- Tecnología debe Implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de la Institución.

## SEGURIDAD EN LOS DESARROLLOS.

Identificar y aprobar antes del desarrollo de sistemas de información, todos los requerimientos de seguridad de la información en la fase de creación del proyecto, los cuales deben estar justificados, aprobados y documentados.

Incluir los requerimientos mínimos de seguridad para desarrollo, infraestructura, servicios y aplicaciones en las implementaciones nuevas, con el fin de tener una metodología propia de desarrollo, con adecuados puntos de control y actividades de seguridad de gestión segura a nivel de versiones y/o configuraciones que mitigan el riesgo, tales como:

- Todo cambio normal y urgente debe pasar por su respectivo control de cambios. Los cambios estándar están definidos previamente y una vez autorizados pueden ejecutarse sin intervención.
- El Director de Desarrollo e Innovación Digital debe identificar los activos de información y los riesgos asociados para nuevos desarrollos o proyectos, con el fin de establecer los controles para el aseguramiento de la información.
- Los datos de salida de los aplicativos que manejan información sensible deben contener los datos relevantes requeridos para el uso de acuerdo con el rol y se deben enviar exclusivamente a los usuarios o terminales autorizadas.
- Los aplicativos de la Institución deben pasar por un proceso de pruebas y aceptación en un ambiente definido para tal fin antes de ser liberados a producción.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- e. El acceso a la información contenida en las bases de datos sólo está permitido a través de las aplicaciones de los sistemas de la Institución. Sólo tienen acceso los usuarios autorizados que de acuerdo con su rol se identifican mediante usuario y contraseña.
- f. La información que está en producción no debe ser utilizada para desarrollo o pruebas, salvo que se realice una copia cambiando toda la información.
- g. Es responsabilidad de los desarrolladores (internos o externos) considerar la seguridad de la información desde el inicio del proceso de diseño de los sistemas de la Institución, pasando por cada una de las fases de desarrollo hasta su liberación a producción.
- h. Los sistemas de procesamiento y almacenamiento de información de los sistemas operativos y aplicaciones deben contar con los últimos parches de seguridad provistos por el fabricante debidamente aprobado e instalado.
- i. No está permitido el acceso a personal no autorizado a editores, compiladores o cualquier otro tipo de utilitarios que estén asociados al ambiente productivo, cuando no sean indispensables para el funcionamiento de este.
- j. Se debe contemplar en el mantenimiento y en la fase de los desarrollos, el establecimiento de buenas prácticas que provean el diseño, aseguramiento y ejecución para la protección de la información a través de buenas prácticas como OWASP, Microsoft SDL, BSIMM.
- k. Los desarrolladores deben generar registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados.
- l. Los desarrolladores deben registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad.

Todo desarrollo debe contar con los siguientes pasos en esquemas de seguridad:

## I. REQUERIMIENTOS GENERALES

- a. Establecer los mecanismos necesarios para asegurar que se realice un análisis de vulnerabilidades de seguridad, estableciendo los controles necesarios para proteger la información sensible o confidencial de la Institución involucrada en un nuevo desarrollo o implementación de un nuevo proyecto.
- b. Definir las métricas al inicio para validar si se debe realizar algún cambio en el proceso de desarrollo, y definir los criterios que deben ser medidos, ya que proporciona visibilidad de los defectos tanto en el proceso del desarrollo, como en el producto final.
- c. Es requisito a nivel de seguridad de desarrollo seguro, comprobar las supuestas vulnerabilidades del código y comprobar si existen deficiencias para realizar los cambios en la fase de diseño, con el fin de no tener inconvenientes en el momento de salir a producción.

## II. REQUERIMIENTOS ESPECÍFICOS

Dentro del desarrollo seguro de aplicaciones se deben tener en cuenta la revisión de los siguientes criterios:

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- Autenticación
- Autorización
- Administración de autenticación y contraseñas
- Gestión de Cookies
- Validación de Entrada de Datos
- Gestión de Errores / Fuga de Información
- Log / Auditoría
- Cifrado de Datos
- Entorno de Código Seguro
- Gestión de Sesiones (Login/Logout)

#### a. Autenticación

Para la autenticación segura se debe tener en cuenta la implementación de controles de autenticación de acuerdo con el riesgo de la aplicación, y otorgar las credenciales individuales dentro del sistema de autenticación con el fin de denegar el acceso a los atacantes.

- Asegurar las peticiones que pasan por un formulario de autenticación, y que éste no se puede saltar.
- Asegurar que las páginas donde se vea involucrada la información corporativa cumplan el requisito de autenticación.
- Asegurar que siempre que se pasen credenciales de autenticación (o cualquier información sensible), sólo se acepte la información vía HTTP POST y nunca con GET.
- Cualquier página para la que se descarte el mecanismo de autenticación, debe ser revisada para asegurarse de que no tenga brechas de seguridad, realizando pruebas de penetración con el fin de que no sea vulnerable o de fácil acceso.
- Asegurar que las credenciales de autenticación no vayan en claro, por tal razón deben ser cifradas.
- Asegurar que no hayan “puertas traseras” en el código de producción, que permitan el acceso de un atacante a las aplicaciones.

#### b. Autorización

- Asegurar que únicamente los usuarios que realicen el acceso a las aplicaciones estén autorizados y con un nivel de privilegio definido dentro de los roles y perfiles estipulados por la Institución, para prevenir ataques de escala de privilegios.
- Asegurar que se tienen mecanismos de autorización (control de acceso y gestión de roles).
- Asegurar que la aplicación tiene claramente definidos los tipos de usuario y sus privilegios.
- Asegurar que se asignan los mínimos privilegios necesarios.
- Asegurar que los mecanismos de autorización funcionan adecuadamente y no pueden saltarse.
- Asegurar la verificación de la autorización en todas las peticiones.
- Asegurar que no hay “puertas traseras” en el código en producción.

#### c. Administración de autenticación y contraseñas

- Asegurar que los usuarios autorizados tengan una autenticación robusta y segura, cumpliendo con los controles de autorización, con el fin de prevenir ataques como la reutilización, falsificación e interpretación de sesiones.
- Requerir autenticación para todos los recursos y páginas excepto aquellas específicamente clasificadas como públicas.
- Establecer y utilizar servicios de autenticación estándares y probados cuando sea posible.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- Utilizar una implementación centralizada para todos los controles de autenticación, incluyendo librerías que llamen a servicios externos de autenticación.
- Segregar la lógica de la autenticación del recurso solicitado y utilizar redirección desde y hacia el control centralizado de autenticación.
- Todos los controles de autenticación deben fallar de una forma segura. La aplicación debe garantizar que, ante una petición transaccional de un atacante, debe arrojar como resultado un error.
- Si la aplicación administra un almacenamiento de credenciales, se debe asegurar que únicamente se almacena el hash con sal (salty hash) de las contraseñas y que el archivo/tabla que guarda las contraseñas y claves solo puede ser escrito por la aplicación (si es posible, no utilizar el algoritmo de hash MD5).
- El hash de las contraseñas debe ser implementado en un sistema en el cual se confíe (Por ejemplo: el servidor).
- Validar los datos de autenticación únicamente luego de haber completado todos los datos de entrada, especialmente en implementaciones de autenticación secuencial.
- Las respuestas a los fallos en la autenticación no deben indicar cual parte de la autenticación fue incorrecta.
- Utilizar autenticación para conexiones a sistemas externos que involucren información o funciones sensibles.
- Las credenciales de autenticación para acceder a servicios externos a la aplicación deben ser encriptados y almacenados en ubicaciones protegidas en un sistema en el cual se confíe. El código fuente NO es una ubicación segura.
- Utilizar únicamente pedidos del tipo HTTP POST para la transmisión de credenciales de autenticación.
- Utilizar únicamente conexiones encriptadas o datos encriptados para el envío de contraseñas que no sean temporales (por ejemplo: correo encriptado). Contraseñas temporales como aquellas asociadas con reseteo por correo electrónico, pueden ser una excepción.
- Hacer cumplir por medio de una política o regulación los requerimientos de complejidad de la contraseña. Las credenciales de autenticación deben ser suficientes como para resistir aquellos ataques típicos de las amenazas en el entorno del sistema. Ej: obligar el uso de combinaciones de caracteres numéricos/alfanuméricos o caracteres especiales de acuerdo con el Manual de Usuario - Cambio de Contraseña.

#### d. Validación de entrada de datos

Garantizar que las aplicaciones sean robustas contra todas las formas de ingreso de datos, ya sea obtenida del usuario, de la infraestructura, de entidades externas o de sistemas de base de datos, ya que nunca se debe confiar en los datos introducidos por cualquier persona, puesto que se tienen muchas posibilidades de manipular los datos.

- Asegurar mecanismos de validación de datos.
- Asegurar la validación de todas las entradas que pueden ser modificadas por un usuario malicioso: cabeceras HTTP, Input fields, hidden fields, drop down lists.
- Asegurar la comprobación de las longitudes de todas las entradas.
- Asegurar la validación de todos los campos, cookies, http headers/bodies y form fields.
- Asegurar la validación de los datos en el servidor.
- Asegurar que no hay “puertas traseras” en el modelo de validación.
- Asegurar que cualquier entrada externa, sea cual sea, sea examinada y validada.

#### e. Gestión de cookies

Proteger las aplicaciones, plataformas o páginas web corporativas con el fin de que no sean vulnerables, por el almacenamiento de datos mediante peticiones entre un ordenador y el servidor corporativo, de donde se puede extraer información sensible para su reutilización y así acceder a los servidores.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- Asegurar que no se puedan hacer operaciones no autorizadas manipulando o sobrescribiendo las cookies.
- Determinar si todas las transiciones de estados en el código de la aplicación verifican el uso seguro de cookies.
- Asegurar la validación de los datos de la sesión.
- Asegurar que las cookies contengan la mínima información privada posible, y que ésta no se vea comprometida. Ej. Usuario y contraseña, permitiendo el secuestro de sesión.
- Asegurar el cifrado de la cookie completa si contiene información privada.
- Definir todas las cookies que usa la aplicación, sus nombres y para qué son necesarias.

#### f. Gestión de errores / Fuga de información

Garantizar que las plataformas sean seguras frente a cualquier tipo de respuesta generada por el desarrollo frente al usuario, donde afecte la integridad de este y permita fuga de información de la Institución.

- Asegurar que todas las llamadas a métodos/funciones que devuelven un valor, tengan un control de errores y además compruebe el valor devuelto.
- Asegurar la gestión adecuada de las excepciones y los errores.
- Asegurar que al usuario no se le devuelven errores del sistema.
- Asegurar que la aplicación falla de un modo seguro.
- Asegurar la liberación de los recursos en caso de error.

#### g. Log / Auditoría

- Asegurar que las aplicaciones bien escritas generen LOGS de doble propósito con trazas de actividad para auditoría y monitoreo, con el fin de identificar una transacción como prueba forense.
- Asegurar que no se registra información privada en el log en caso de error.
- Asegurar que se define y controla la longitud máxima de una entrada de log.
- Asegurar que no se registran datos sensibles en el log: cookies, método HTTP "GET", credenciales de autenticación.
- Determinar si la aplicación auditará las operaciones lanzadas desde el cliente, sobre todo la manipulación de datos: Insert, Create, Update, Delete (operaciones CUD), Grant, Deny, Alter.
- Asegurar el registro en el log de las operaciones de autenticación (fallidas o exitosas).
- Asegurar el registro en el log de los errores de la aplicación.
- Determinar si al hacer debug se están registrando datos privados en el log.
- Deshabilitar el botón derecho del copy/paste.

#### h. Cifrado de datos

- Asegurar el cifrado de la información para proteger la confidencialidad e integridad de los datos privados o sensibles de los usuarios o de la Institución.
- Asegurar que no se transmiten datos sensibles en claro, interna o externamente.
- Asegurar que la aplicación implementa buenos y conocidos métodos criptográficos.

#### i. Entorno de código seguro

- Asegurar el entorno de las aplicaciones con el fin de reducir la probabilidad de un ataque, dado que los códigos tienen vulnerabilidades que ponen en riesgo las plataformas del negocio y representan un riesgo.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- Examinar en la estructura de archivos si hay algún componente que no debe estar directamente accesible para los usuarios.
- Comprobar la gestión de memoria (reservar/liberar).
- Comprobar si la aplicación usa SQL dinámico y determinar si es vulnerable a inyecciones de código.
- Comprobar si la aplicación tiene funciones “main()” ejecutables y depurar “puertas traseras”.
- Buscar código comentado (aunque sea para pruebas) que pueda contener información sensible.
- Asegurar que todas las ramificaciones de código tengan su cláusula default (if-else, switch-default, etc).
- Asegurar que no hay “development environment kits” en los directorios en explotación.
- Buscar llamadas al sistema operativo, así como aperturas de archivos, y comprobar las posibilidades de error.

#### j. Gestión de Sesiones (Login / Logout)

- Asegurar o controlar el acceso o salida individual al sistema informático, mediante las credenciales del usuario de forma segura.
- Comprobar cómo y cuándo se crean las sesiones de usuario, ya sean autenticadas o no.
- Comprobar el ID de sesión y verificar que tiene la complejidad necesaria para “ser fuerte”.
- Comprobar cómo se almacenan las sesiones: en base de datos, en memoria, etc.
- Comprobar cómo la aplicación hace el seguimiento de las sesiones (track sessions).
- Determinar qué hace la aplicación en caso de encontrar un ID de sesión inválido.
- Comprobar la invalidación de sesiones.
- Determinar cómo se gestionan las sesiones multithreaded/multi-user.
- Determinar el timeout de inactividad de la sesión HTTP.
- Determinar cómo funciona el log-out

#### k. Evaluación vulnerabilidades

Los requerimientos de seguridad del diseño y desarrollo e implantación de nuevas aplicaciones se deben realizar mediante un análisis de vulnerabilidades que pueden ser aprovechadas por las amenazas del ambiente o escenario en el cual se desarrolle o implemente la solución.

Esta evaluación debe ser realizada por especialistas en pruebas de intrusión o seguridad informática, independiente del área de Tecnología y preferiblemente en ambientes de Calidad.

Como punto de referencia para realizar el análisis, el Politécnico Grancolombiano se rige bajo la metodología documentada en el Top 10 de riesgos reportados por el grupo OWASP (OWASP Top 10 2013- Ten most critical web security application risk).

|                                                    |                             |                                                                |                                                     |
|----------------------------------------------------|-----------------------------|----------------------------------------------------------------|-----------------------------------------------------|
| <b>PROCESO:</b><br>Mencionar el nombre del proceso | <b>POLÍTICA</b>             | <b>Acuerdo - Resolución:</b> Registrado por secretaría general | <b>Código:</b> Registrado por el sistema integrado  |
|                                                    | <b>NOMBRE DEL DOCUMENTO</b> | <b>Fecha aprobación:</b> Registrado por secretaría general     | <b>Versión:</b> Registrado por el sistema integrado |

|                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>A1- Inyección</b>                                                  | Las fallas de inyección, tales como SQL, OS, y LDAP, ocurren cuando datos no confiables son enviados a un interprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al interprete en ejecutar comandos no intencionados o acceder datos no autorizados.                                                                                                                                                                |
| <b>A2 – Pérdida de Autenticación y Gestión de Sesiones</b>            | Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son frecuentemente implementadas incorrectamente, permitiendo a los atacantes comprometer contraseñas, claves, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios.                                                                                                                                                   |
| <b>A3 – Secuencia de Comandos en Sitios Cruzados (XSS)</b>            | Las fallas XSS ocurren cada vez que una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada. XSS permite a los atacantes ejecutar secuencia de comandos en el navegador de la víctima los cuales pueden secuestrar las sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso.                                                                                    |
| <b>A4 – Referencia Directa Insegura a Objetos</b>                     | Una referencia directa a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, tal como un fichero, directorio, o base de datos. Sin un chequeo de control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder datos no autorizados.                                                                                                                                   |
| <b>A5 – Configuración de Seguridad Incorrecta</b>                     | Una buena seguridad requiere tener definida e implementada una configuración segura para la aplicación, marcos de trabajo, servidor de aplicación, servidor web, base de datos, y plataforma. Todas estas configuraciones deben ser definidas, implementadas, y mantenidas ya que por lo general no son seguras por defecto. Esto incluye mantener todo el software actualizado, incluidas las librerías de código utilizadas por la aplicación.            |
| <b>A6 – Exposición de datos sensibles</b>                             | Muchas aplicaciones web no protegen adecuadamente datos sensibles tales como números de tarjetas de crédito o credenciales de autenticación. Los atacantes pueden robar o modificar tales datos para llevar a cabo fraudes, robos de identidad u otros delitos. Los datos sensibles requieren de métodos de protección adicionales tales como el cifrado de datos, así como también de precauciones especiales en un intercambio de datos con el navegador. |
| <b>A7 – Ausencia de Control de Acceso a Funciones</b>                 | La mayoría de aplicaciones web verifican los derechos de acceso a nivel de función antes de hacer visible en la misma interfaz de usuario. A pesar de esto, las aplicaciones necesitan verificar el control de acceso en el servidor cuando se accede a cada función. Si las solicitudes de acceso no se verifican, los atacantes podrán realizar peticiones sin la autorización apropiada.                                                                 |
| <b>A8 - Falsificación de Peticiones en Sitios Cruzados (CSRF)</b>     | Un ataque CSRF obliga al navegador de una víctima autenticada a enviar una petición HTTP falsificado, incluyendo la sesión del usuario y cualquier otra información de autenticación incluida automáticamente, a una aplicación web vulnerable. Esto permite al atacante forzar al navegador de la víctima para generar pedidos que la aplicación vulnerable piensa son peticiones legítimas provenientes de la víctima.                                    |
| <b>A9 – Utilización de componentes con vulnerabilidades conocidas</b> | Algunos componentes tales como las librerías, los frameworks y otros módulos de software casi siempre funcionan con todos los privilegios. Si se ataca un componente vulnerable esto podría facilitar la intrusión en el servidor o una pérdida seria de datos. Las aplicaciones que utilicen componentes con vulnerabilidades conocidas debilitan las defensas de la aplicación y permiten ampliar el rango de posibles ataques e impactos.                |
| <b>A10 – Redirecciones y reenvíos no validados</b>                    | Las aplicaciones web frecuentemente redirigen y reenvían a los usuarios hacia otras páginas o sitios web, y utilizan datos no confiables para determinar la página de destino. Sin una validación apropiada, los atacantes pueden redirigir a las víctimas hacia sitios de phishing o malware, o utilizar reenvíos para acceder páginas no autorizadas.                                                                                                     |

## SEGURIDAD PARA LOS PROVEEDORES, CONTRATISTAS Y TERCEROS.

- Los proveedores, contratistas o terceros vinculados al Politécnico Grancolombiano deben garantizar que el intercambio de información desde y hacia la Institución cumpla con las exigencias institucionales definidas con base en las leyes y regulaciones vigentes, así como también las disposiciones de la presente política.
- Los proveedores o contratistas deben informar inmediatamente al Politécnico Grancolombiano de cualquier incidente que afecte la confidencialidad, integridad y disponibilidad de los activos de información que ponga en riesgo la operación de la Institución.
- Los proveedores y contratistas vinculados al Politécnico Grancolombiano que tengan acceso a la información reservada de la Institución deben firmar un acuerdo de confidencialidad o debe incluirse una cláusula de confidencialidad al correspondiente contrato con el fin de proteger dicha información.
- En el contrato de servicios se debe incluir una cláusula de confidencialidad y niveles de servicios en seguridad de la información, que detalle sus compromisos en el cuidado de esta y consecuencias contractuales, indemnizaciones,

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

multas o sanciones previstas en el contrato la pena a que estaría sujeto el Proveedor o Contratista en caso de incumplirlos. Los proveedores que tengan acceso a información confidencial deben protegerla y resguardarla.

- e. El cumplimiento de los acuerdos mencionados anteriormente debe ser verificado periódicamente por el Director de Gobierno Digital y la Dirección Jurídica.
- f. Cada relación con un tercero sea o no una empresa relacionada con el Politécnico Grancolombiano, debe tener un representante o interventor facultado por la Institución, que sea responsable durante toda la vigencia del contrato de monitorear el cumplimiento de los compromisos adquiridos frente a la seguridad, el correcto uso y la protección adecuada de la información de la Institución a la cual tiene acceso el tercero.
- g. Abstenerse de divulgar en cualquier forma o de utilizar en provecho propio o ajeno, la información de carácter confidencial o restringida que se haya conocido en ejercicio de sus funciones.
- h. Cumplir con las disposiciones legales aplicables, así como aquellas normas internas adoptadas en materia de seguridad de la información.
- i. Los proveedores que administren, procesen o tengan acceso a sistemas de información institucionales deberán implementar controles y buenas prácticas de seguridad de la información acordes con la naturaleza de los servicios prestados y los riesgos identificados.
- j. Responder adecuadamente por los activos asignados y los de la Institución.
- k. Cumplir con la política de tratamiento de los datos personales y los estándares definidos para la correcta recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales.
- l. Asegurar la protección de la confidencialidad, integridad y disponibilidad de los activos de información proporcionados como parte del objeto del contrato u orden de compra. Notificar los incidentes de seguridad de forma inmediata, una vez se tenga conocimiento de estos, gestionarlos y reportar el plan de tratamiento correspondiente.
- m. Informar oportunamente cualquier cambio o modificación en el servicio que pueda afectar la información.

## ADMINISTRACIÓN DE PORTALES.

Para efectos de la presente política, se entiende por portal institucional cualquier sitio web, plataforma digital, micrositio, aplicación web o entorno electrónico administrado por el Politécnico Grancolombiano que permita la consulta, publicación, intercambio o procesamiento de información institucional o de usuarios.

La administración de portales establece los lineamientos orientados a garantizar la disponibilidad, integridad, confidencialidad y adecuada protección de la información publicada o gestionada a través de dichos entornos digitales, conforme a las políticas y controles de seguridad de la información definidos por la Institución.

- a. Los portales deben tener publicado en su “home” la Política de Seguridad de la Información con alusión al uso de los activos de información de la Institución, la cual debe ser de conocimiento de los estudiantes y su aplicación es obligatoria.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- b. Todos los portales deben exigir a los estudiantes cambiar la contraseña cada 30 días, con el fin de evitar accesos no autorizados.
- c. Los portales de la Institución deben contar con un disclaimer que comunique las políticas de seguridad.
- d. Los empleados, estudiantes y terceros deben utilizar los sistemas de información y comunicación dispuestos por el Politécnico Grancolombiano solo para los fines de consulta que estos brindan y bajo ningún aspecto se debe tratar de ingresar a la red para consultar material ilegal, de acoso, difamatorio, abusivo, amenazador, nocivo, vulgar, intrusivo, obsceno o de cualquier otra manera censurable, o a la información de la Institución para borrar, capturar, modificar o cualquier otra manifestación que esté en contra de las políticas aquí definidas y por la legislación Colombiana vigente.

#### INCIDENTES DE SEGURIDAD.

- a. Las personas involucradas que utilicen servicios de información del Politécnico Grancolombiano deben reportar cualquier sospecha de amenazas o debilidades en los sistemas o servicios de la Institución de forma inmediata. Dichos reportes deben ser comunicados a la Gerencia de Tecnología e Innovación Digital.
- b. Los incidentes de seguridad que afecten los activos de información deben ser manejados con la participación de la Mesa de Soluciones, por lo cual queda expresamente prohibido divulgarlos a personal no autorizado, a menos que haya sido formalmente autorizado por la Gerencia de Tecnología e Innovación Digital y ésta tenga conocimiento de la situación.
- c. Se debe reportar a la Mesa de Soluciones cualquier incidente de seguridad que pueda comprometer la confidencialidad, integridad o disponibilidad de los activos de información de la Institución, según lo dispuesto en el Procedimiento - Gestión de Activos de Información.

#### CONTINUIDAD.

- a. La Gerencia de Planeación Estratégica realizará un Plan de Continuidad en la Institución el cual estará disponible en el CIO - Centro de Información de la Organización, basado en los siguientes aspectos:
  - Entender los riesgos que enfrenta la Institución y su impacto, incluyendo la identificación y sensibilidad de sus procesos críticos.
  - Entender el impacto de las interrupciones o incidentes de seguridad en las actividades de la Institución.
  - Formular y documentar planes estratégicos de continuidad de la Institución acorde con los objetivos y prioridades del Politécnico Grancolombiano.
- b. La Institución deberá ejecutar periódicamente pruebas de recuperación ante desastres, restauración de respaldos y respuesta a incidentes de ciberseguridad, documentando los resultados, las oportunidades de mejora y los planes de acción derivados de cada ejercicio.

#### CUMPLIMIENTO REGULATORIO.

- a. La Institución vela por el cumplimiento de la presente política y la legislación aplicable vigente por los entes de control.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b><br><i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|---------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b><br><i>Registrado por secretaría general</i>  | <b>Versión:</b><br><i>Registrado por el sistema integrado</i> |

- b. La Gerencia de Tecnología e Innovación Digital en conjunto con la Dirección Jurídica, mediante la identificación de requisitos de seguridad de la información que sean de cumplimiento obligatorio y emitidos por entes gubernamentales o privados y cualquier disposición colombiana vigente, definen e implementan los controles necesarios para dar cumplimiento y protección a los activos de información.
- c. La titularidad y transferencia de los derechos de propiedad intelectual sobre obras, desarrollos, invenciones y demás resultados creados en ejecución de contratos de trabajo o de prestación de servicios se registrará por la normativa aplicable, la Política de Propiedad Intelectual y Transferencia de Conocimiento y los acuerdos escritos celebrados con la Institución. En materia de derecho de autor, el autor conservará sus derechos morales y, salvo pacto en contrario, los derechos patrimoniales se presumirán transferidos al empleador o contratante en la medida necesaria para el ejercicio de sus actividades habituales, siempre que el contrato conste por escrito. En materia de propiedad industrial se aplicarán las reglas legales de titularidad y transferencia correspondientes, sin perjuicio de los pactos en contrario. Las aplicaciones, contenidos y desarrollos de terceros se registrarán por las licencias y contratos respectivos.
- d. El Politécnico Grancolombiano se reserva el derecho de monitorear los computadores que sean de su propiedad y estén conectados o no a la red de la Institución. En caso de presentarse incidentes que afecten la seguridad de la información de la Institución, siempre con el seguimiento del debido proceso y el derecho a la intimidad de sus empleados.
- e. Aquellos documentos que estén bajo lineamientos legales o regulatorios deben ser resguardados bajo las medidas de seguridad adecuadas para garantizar su integridad y en general el cumplimiento con las disposiciones legales y regulatorias.
- f. La Gerencia de Tecnología e Innovación Digital debe revisar periódicamente los acuerdos de licencias de hardware y software instalado a fin de verificar el cumplimiento de estos por parte de la Institución.
- g. Los contratistas y terceras partes deben cumplir con las disposiciones establecidas por la Legislación Colombiana vigente asociados a la de protección de datos personales, propiedad intelectual y seguridad de la información.
- h. El incumplimiento de las obligaciones y responsabilidades previstas en esta política podrá dar lugar a la adopción de las medidas académicas, disciplinarias, contractuales, administrativas o legales que resulten procedentes, según la naturaleza del vínculo, la gravedad de la conducta y las circunstancias particulares del caso, de conformidad con el Reglamento Interno de Trabajo, los contratos y la normatividad aplicable, y con observancia del debido proceso. La calificación de una conducta como falta grave se determinará únicamente cuando así proceda conforme a las fuentes legalmente habilitadas.
- i. Desde el punto de vista de cumplimiento normativo el Politécnico Grancolombiano debe tener presente la ley 1581 de 2012 de Protección de Datos Personales, así como las buenas prácticas en el cumplimiento de estándares, normas y regulaciones como ISO27001, PCI-DSS, además de las políticas definidas por la Institución.
- j. El estudio de la normatividad publicada por organismos del estado inherente a Seguridad de la Información es una actividad permanente en conjunto con la Dirección Jurídica y de Gobierno Digital, con el fin de garantizar su aplicación adecuada y oportuna para la Institución.
- k. El Director de Gobierno Digital, se comunicará con la Dirección Jurídica, cuando tenga conocimiento de una nueva legislación aplicable a cualquiera de los procesos de la Institución con respecto a seguridad de la información.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- I. El Director de Gobierno Digital es el responsable de gestionar y hacer seguimiento a la implementación de las normas nacionales que apliquen a la seguridad de la información.
- m. Todos los procesos y operaciones de la Institución deben regirse por la legislación colombiana vigente respecto a seguridad de la información.

## CIFRADO O ENCRIPCIÓN DE MEDIOS.

- a. Los mecanismos de cifrado de información deberán evaluarse para su aplicación en: discos duros de portátiles, servidores de archivos o file servers, cintas o medios de respaldo de información, memorias USB y discos externos.
- b. Toda información con alto valor a la Institución no debe ser transferida empleando canales no seguros como la internet; ésta deberá ser cifrada y para el envío deberá emplearse un medio como la ZTNA para la transmisión. Se debe evitar el uso de protocolos como ftp en caso de que la información no se encuentre cifrada.
- c. El correo electrónico corporativo debe estar integrado con mecanismos de cifrado por intercambio de llaves públicas y privadas para el envío de correos confidenciales o de alto valor para la Institución.
- d. Toda información o medio de almacenamiento con un valor Alto para la Institución, bien sea por su nivel de confidencialidad, disponibilidad o integridad, deberá ser evaluado entre el Director de Gobierno Digital y los dueños de los activos para decidir si se aplicará un mecanismo de cifrado.
- e. El Área de Tecnología debe establecer el esquema tecnológico para cifrar la información, definir si el activo requiere ser reubicado para su aislamiento y posterior cifrado, ejecutar el cifrado de la información y configurar los accesos a la información cifrada.
- f. El Área de Tecnología, bajo los lineamientos del Director de Gobierno Digital, serán custodios de las claves, software de cifrado y certificados electrónicos, dependiendo el método de cifrado a implementarse.
- g. El dueño de un activo es el responsable de comunicar al Director de Gobierno Digital, la necesidad del cifrado de información para que sea evaluado en conjunto. Esta actividad aplica para toda nueva información que no haya sido clasificada y valorada previamente.
- h. La distribución de las llaves criptográficas se debe limitar a la entrega de la llave de acceso al usuario y a la notificación al dueño de la información, ya que las llaves de recuperación serán responsabilidad directa del custodio de llaves.
- i. El Director de Gobierno Digital es el responsable de definir los controles de custodia de llaves criptográficas, así como el Área de Tecnología es responsable de hacer cumplir los controles de seguridad definidos, la custodia de las llaves criptográficas y distribución segura de las mismas.

## 6.2 SEGUIMIENTO

El seguimiento a la implementación de la Política será realizado por las dependencias responsables, de acuerdo con sus competencias y con el modelo institucional de gestión de Seguridad de la Información.

El seguimiento comprenderá, entre otros aspectos:

- Cumplimiento de los lineamientos establecidos en la Política.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b> <i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b> <i>Registrado por secretaría general</i>     | <b>Versión:</b> <i>Registrado por el sistema integrado</i> |

- Estado de implementación de los controles.
- Gestión de activos de información.
- Clasificación y valoración de activos.
- Gestión de riesgos.
- Gestión de accesos y privilegios.
- Revisión de cuentas de usuario.
- Cumplimiento de controles de seguridad en servicios tecnológicos y nube.
- Gestión y tratamiento de incidentes.
- Resultados de análisis e investigaciones.
- Cumplimiento de los requisitos de seguridad de proveedores.
- Actividades de capacitación y sensibilización.
- Resultados de auditorías.
- Estado de las acciones correctivas y de mejora.

Para el seguimiento podrán establecerse indicadores relacionados con:

- Número y criticidad de incidentes de seguridad.
- Tiempo de detección y atención de incidentes.
- Cumplimiento de revisión de accesos.
- Cumplimiento de gestión de activos.
- Porcentaje de usuarios capacitados.
- Cumplimiento de controles de seguridad.
- Vulnerabilidades identificadas y gestionadas.
- Cumplimiento de planes de tratamiento de riesgos.
- Cumplimiento de planes de mejoramiento.

### 6.3 EVALUACIÓN Y MEJORAMIENTO CONTINUO

La Institución realizará evaluaciones periódicas de la Política, del Sistema de Gestión de Seguridad de la Información y de los controles asociados, mediante auditorías, revisiones, evaluaciones de riesgos, análisis de incidentes, indicadores y demás mecanismos definidos institucionalmente.

Las auditorías podrán ser internas o externas y deberán realizarse bajo criterios previamente establecidos, garantizando, cuando corresponda, independencia y objetividad.

Los resultados de auditoría deberán documentarse mediante las evidencias correspondientes y permitirán identificar conformidades, incumplimientos, oportunidades de mejora, riesgos y necesidades de fortalecimiento de los controles. Los resultados de los incidentes de seguridad deberán utilizarse como insumo para la mejora continua y para la actualización de controles, procedimientos, capacitaciones y demás mecanismos de protección.

Cuando se identifiquen desviaciones, incumplimientos o riesgos que requieran intervención, se deberán establecer los planes de mejoramiento o acciones correctivas y preventivas correspondientes, indicando responsables y mecanismos de seguimiento.

La Política deberá ser revisada y actualizada cuando se presenten cambios:

- Normativos.
- Regulatorios.

| <b>PROCESO:</b><br><i>Mencionar el nombre del proceso</i> | POLÍTICA             | <b>Acuerdo - Resolución:</b> <i>Registrado por secretaría general</i> | <b>Código:</b><br><i>Registrado por el sistema integrado</i>  |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------------------------|---------------------------------------------------------------|
|                                                           | NOMBRE DEL DOCUMENTO | <b>Fecha aprobación:</b><br><i>Registrado por secretaría general</i>  | <b>Versión:</b><br><i>Registrado por el sistema integrado</i> |

- Tecnológicos.
- Organizacionales.
- Operacionales.
- En los riesgos institucionales.
- En los procesos institucionales.
- En los marcos o buenas prácticas adoptadas por la Institución.

La evaluación y mejoramiento continuo deberán orientarse a mantener la eficacia de los controles y la capacidad institucional para prevenir, detectar, responder y recuperarse frente a eventos e incidentes de Seguridad de la Información.