PROCESO: Gestión de Recursos Tecnológicos	**POLÍTICA**	**Código:** TI-POL-001
	SEGURIDAD DE LA INFORMACIÓN	**Versión:** 4

1. OBJETIVO

Establecer los criterios y medidas básicas que deben aplicarse a la información Institucional para su correcto uso, manteniendo un ambiente controlado y fuera de riesgos.

2. ALCANCE

Aplica a todos los procesos de la Institución, estudiantes, 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.

3. DEFINICIONES

- **Activo de información**: Objetos materiales o intangibles, tales como bases de datos, contratos, manuales de usuario, aplicaciones o softwares asociados con la información y que son requeridos para las actividades institucionales, siendo clasificados de acuerdo con su criticidad e importancia para la Institución.
- **Alcance de la auditoria:** Extensión y límites de una auditoria para el SGSI.
- **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.
- **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.
- **Building Security In Maturity Model (BSIMM)**: Sistema diseñado para ayudar, comprender, medir y planificar una iniciativa de seguridad del software.
- **Buzón de Correo:** Corresponde al repositorio local o en servidor donde se localizan los correos electrónicos de una persona o empleado.
- **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.
- **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.
- **Demoware:** Tipo de software comercial que generalmente permite su uso sin ninguna restricción por un período limitado de tiempo (o alguna otra limitación), y que luego de terminado ese período, deshabilita ciertas funciones. Algunas limitaciones son: poder ser ejecutados en un período determinado de veces, no permitir guardar los proyectos en archivos, entre otros.
- **Disclaimer:** Advertencias (warnings) unilaterales dirigidas al público en general.
- **Disponibilidad de la información**: Acceso oportuno y confiable del uso de la información de la Institución.
- **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 del mismo.

- **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.

- **Freeware:** Tipo de software que se distribuye sin costo, disponible para su uso y por tiempo ilimitado, siendo una variante gratuita del shareware, en el que la meta es lograr que un usuario pruebe el producto durante un tiempo limitado, y si le satisface, pagándolo, se habilitan todas sus funciones.

- **File Server**: Repositorio asignado a un proceso para guardar información.

- **Form fields:** Campos de formularios**.**

- **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.

- **Http bodies:** Bytes de datos transmitidos en un HTTP.

- **Http headers:** Protocolo que usa todo internet para las comunicaciones.

- **Información vía GET:** Información obtenida del servidor. En otras palabras, son datos alojados en un servidor, ya sea en un archivo o base de datos, y que son transmitidos al cliente.

- **Información vía HTTP POST:** Información enviada desde el cliente para que sea procesada y actualice o agregue información en el servidor.

- **Integridad de la Información**: Protección de la información que asegura su exactitud o completitud, manteniendo intacta su estructura desde el punto de envío hasta el destino final.

- **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.

- **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.

- **Microsoft SDL Security Development Lifecycle (SDL**): Sistema que ayuda a los desarrolladores a crear software y requisitos de cumplimiento de seguridad de direcciones más seguras al tiempo que reduce los costes del desarrollo.

- **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.

- **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.[1]

- **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.

- **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 (autentificación) para acceder al sistema.

- **Riesgo**: Medida de la magnitud de los daños frente a una situación peligrosa. El riesgo se mide asumiendo una determinada vulnerabilidad o amenaza frente a cada tipo de peligro, así como su probabilidad de ocurrencia y el impacto del mismo en la Institución.

- **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:

---

1 Para más información consultar www.owasp.org

- La confidencialidad
- La disponibilidad
- La integridad

- **Shareware:** Modalidad de distribución de software, en la que el usuario puede evaluar en forma gratuita el producto, pero con limitaciones en el tiempo de uso o en algunas de las formas de uso o con restricciones en las capacidades finales.

- **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 pueden 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.

- **Trialware**: Programas que permiten su utilización completa al usuario, pero solo por un determinado período de tiempo. A diferencia de los demás, los trialwares, se pueden utilizar una vez.

- **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. LINEAMIENTOS

4.1. Declaración de la Política

a. 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 les haya autorizado el acceso a la información, serán responsables por el buen uso que se le dé a la misma.

b. El Comité Ejecutivo expresa su compromiso con la Seguridad de la Información al establecer la presente política y al apoyar todas las iniciativas encaminadas a cumplir con los lineamientos aquí establecidos.

c. La verificación de la aplicación de la Política de Seguridad de la Información y sus actualizaciones está a cargo del Director de Seguridad y Activos de Información. El Comité Ejecutivo y cada uno de los empleados aseguran que la política esté alineada con la estrategia institucional.

d. 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.

e. La Gerencia de Tecnologías de la Información y Comunicaciones es 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.

f. Todo estudiante, empleado, contratista o quien tenga vínculo contractual con la Institución está obligado a conocer, entender, cumplir las normas y disposiciones de la presente política, para el buen manejo de la protección de la información y de la infraestructura tecnológica con el objetivo de asegurar su confidencialidad, integridad y disponibilidad.

g. 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 Grancolombiano, 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.

h. El incumplimiento de las políticas aquí expresadas, acarrearán las acciones disciplinarias que determine la Gerencia de Gestión Humana.

4.2. Responsabilidades de los empleados

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.

a. El Director de Seguridad y Activos de Información**:** Es el responsable de impulsar la implementación y cumplimiento de la presente Política. También es responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la Institución.

b. Los propietarios de activos de información: tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo, mientras sea desarrollado, producido, mantenido y utilizado.

4.3. Seguridad de los recursos humanos

a. Todos los empleados deben cumplir con el Procedimiento - Selección, Contratación y Promoción de Personal definido por la Gerencia de Gestión Humana.

b. Todos los empleados y terceros vinculados a la Institución deben firmar un acuerdo de confidencialidad que tiene como finalidad dar a conocer las obligaciones, compromisos y responsabilidades que tiene el personal en cuanto al manejo de la información se refiere.

c. 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 pendrive, discos duros, equipos de cómputo, servidores, bases de datos, entre otros. El Auxiliar de Activos Fijos en conjunto con el Jefe de Área son los responsables de recibir dichos activos.

4.4. Seguridad de activos de información

a. 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 Seguridad y Activos de Información, quien se va a encargar de actualizarlo cuando sea necesario.

b. Los activos de información de la Institución deben estar salvaguardados según su nivel de criticidad.

c. 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.

d. Ningún estudiante, empleado o tercero vinculado al Politécnico Grancolombiano 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 - Gestión de Activos de Información.

f. Los activos de información que deban ser enviados o compartidos deben estar etiquetados 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 Tecnologías de la Información y Comunicaciones.

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 es una responsabilidad del propietario del activo de información y los custodios.

4.5. Seguridad en el control de acceso lógico

a. 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.

b. 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.

c. 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.

d. 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.

e. 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.

f. 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.

g. 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.

h. 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 Tecnologías de la Información y Comunicaciones.

i. 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.

j. Todas las aplicaciones de la Institución deberán ser autenticadas contra el directorio activo, a excepción de ERP SAP

k. El campo de contraseña debe estar parametrizado con las siguientes opciones:

- La longitud mínima es de 8 caracteres
- La vigencia de las contraseñas es de 120 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:
    - Una mayúscula
    - Una minúscula
    - Un carácter especial (+*/_ {)
    - Un número

l. Las cuentas de usuarios nunca deben estar marcadas con "Password Never Expires" a excepción de las de servicio.

m. Se prohíbe almacenar sin cifrar, usuarios y contraseñas de acceso a las aplicaciones de la Institución en cualquier medio físico, magnético o electrónico.

n. Cada 6 meses se realizará depuración de usuarios y se deshabilitarán las cuentas de estudiantes que no hayan tenido ningún tipo de actividad.

4.6. 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. 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.

c. No se permite el uso o envío del correo electrónico para actividades personales, comerciales, mensajes en cadena que contengan bromas, advertencias de software malicioso, mensajes con contenido religioso, de juegos, racista, sexista, pornográfico, publicitario no corporativo, político, mensajes mal intencionados o cualquier otro tipo de mensajes que no estén autorizados, atenten contra la dignidad de las personas o que comprometan de alguna forma los activos de información de la Institución.

d. 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 Gerencia de Comunicaciones Intregradas, Rectoría y SEGE.

e. Las cuentas de servicio de la Institución como son las de Huella Grancolombiana, SEGE, movilidad, prácticas empresariales, becas y monitorias, responsabilidad social, realizan envíos de información institucional cumpliendo las recomendaciones de tratamiento de datos personales.

f. Las cuentas de servicio que manejan los CSU, tienen comunicación personalizada con los usuarios y cumple con las recomendaciones de tratamiento de datos personales.

g. 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.

h. El correo electrónico debe ser manejado como una comunicación directa entre un remitente y un destinatario autorizado. En tal sentido, las personas involucradas no deben utilizar cuentas de correo electrónico asignadas a otra persona para enviar o recibir mensajes.

i. 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 Tecnologías de la Información y Comunicaciones.

4.6.1. Revisión de cuentas de correo electrónico

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. Los analistas de servidores deberán monitorear periódicamente 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. Tecnología se reserva el derecho de retirar el servicio con previo aviso, ante violaciones del código de ética, reglamento o políticas institucionales de seguridad de la información.

f. Se le deberá informar al Director de Seguridad y Activos de Información 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.

g. El Director de Seguridad y Activos de Información 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 Tecnologías de la Información y Comunicaciones sobre los resultados de su investigación para su posterior notificación a Gestión Humana.

h. El Director de Seguridad y Activos de Información debe generar un informe a nivel forense, con el fin de definir el mayor tipo de evidencias recaudadas y que demuestren la acción intencional de un usuario respecto al mal uso de los activos de información.

4.7. 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 Tecnología.

f. Todos los colaboradores tendrán internet básico, 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.

4.8. 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 Tecnologías de la Información y Comunicaciones. Las únicas áreas para utilizar discos externos de gran capacidad son Centro de Medios, Departamento de Comunicaciones y 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 Tecnologías de la Información y Comunicaciones.

c. No está autorizado el uso de recursos informáticos (datos, hardware, software, redes, servicios) y de telecomunicaciones (teléfono, fax) 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 Tecnologías de la Información y Comunicaciones

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.

4.9. Dispositivos móviles

a. Todo dispositivo móvil (tablets, teléfonos inteligentes, laptops, 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. Los equipos críticos definidos (rector, vicerrector, gerentes, directores y decanos) por la Institución que contengan información confidencial debe contar con el cifrado de su disco duro de acuerdo con lo dispuesto en la Política - Cifrado de Información.

c. 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.

d. 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 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.

e. No está permitido el uso de equipos móviles personales, dentro de la red ADMINISTRATIVA y VIP, salvo si existe una autorización por el Jefe Inmediato informando la novedad del uso de este.

f. Para los estudiantes que hacen parte del programa de INCLUSION EDUCATIVA, se habilitará el acceso con los mismos privilegios de la red VIP.

g. Las personas que tienen asignados equipos que son propiedad de la Institución y deseen adherirle calcomanías, solo serán permitidas las que ofrece el área de Tecnología; y ellos serán los designados para informar donde se deberán colocar.

4.10. Teletrabajo

a. Los usuarios que por razones propias de la Institución se encuentren autorizados para realizar teletrabajo, son responsables por la protección física del equipo asignado contra acceso, uso no autorizado, hurto, pérdida o daño de información confidencial institucional.

b. Las conexiones que se realicen desde y hacia los equipos destinados para teletrabajo, se deben hacer a través de VPN con el fin de dar aseguramiento a los activos de información de la Institución.

c. La Gerencia de Tecnologías de la Información y Comunicaciones 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.

4.11. Sistemas de Información

a. La Gerencia de Comunicaciones Integradas, 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 Gerencia de Comunicaciones Integradas es la única autorizada para publicar información, crear usuarios en redes sociales, blogs, usar logos o cualquier otro tipo de contenido a nombre de la Institución.

c. Toda instalación, configuración, mantenimiento y actualización de hardware y software debe ser realizada por la Gerencia de Tecnologías de la Información y Comunicaciones a excepción de las personas que cuentan con autorización por parte del Responsable del Área.

4.12. 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. Solamente está permitido el aseo para el bloque C, donde está ubicado el DATA CENTER primer sector; por ningún motivo personal ajeno a la Gerencia de Tecnologías de la Información y Comunicaciones (personal autorizado) debe ingresar al lugar donde están ubicados los servidores y equipos de comunicaciones.

e. El acceso físico a los centros de procesamiento de datos y cableado de todas las sedes es responsabilidad de la Gerencia de Tecnologías de la Información y Comunicaciones.

f. 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.

g. 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.

h. Todo el personal vinculado a la Institución debe portar en un lugar visible y en todo momento el carné institucional que los identifique.

i. 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.

j. 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.

k. El ingreso a las sedes de la institución se permite en el siguiente horario:
   - Lunes a viernes de 6:00 a.m. a 9:59 p.m.
   - Sábado de 6:30 a.m. a 3:59 p.m.

   Toda persona que desee ingresar a las instalaciones fuera de las horas indicadas, debe enviar un correo de solicitud con la hora de ingreso y su respectiva justificación al Jefe Administrativo al menos con un día hábil de anticipación a la fecha de entrada a autorizar. Una vez aprobado, se debe informar del ingreso al personal designado por parte del Coordinador de Seguridad de la Institución quién gestiona el permiso que corresponde con el personal de seguridad en la sede en donde se ha autorizado el ingreso. Al personal que no esté relacionado en el formato aprobado, no se le permite el acceso en ninguna circunstancia, exceptuando cuando se presente una falla en los equipos de cómputo críticos que necesitan atención inmediata por parte del personal de Infraestructura TI, para lo cual no es necesario el envío de autorización, pero si se debe dejar por escrito la novedad.

l. Para el caso de activos fijos propiedad de la Institución que se encuentren extraviados, el Jefe Administrativo o el Coordinador de Seguridad debe entregar a Activos Fijos el elemento encontrado, relacionándolo en una planilla simple remitida por correo electrónico.

m. Los equipos tecnológicos se almacenan en bodegas destinadas para tal efecto, bajo la responsabilidad de la Gerencia de Tecnologías de la Información y Comunicaciones.

n. 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.

o. 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. Es responsabilidad de cada uno de los procesos, notificar al Coordinador de Seguridad la ubicación de dichos elementos y asignar el presupuesto suficiente para establecer los controles necesarios.

p. Es responsabilidad de cada uno de los procesos establecer los controles físicos necesarios que establezca la Coordinación de Seguridad dentro de su análisis de riesgos.

q. Los computadores y fotocopiadoras 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.

4.13. 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 Redes y Servidores 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.

4.14. Instalación y uso de software

a. Todas las adquisiciones de software deben estar avaladas por la Gerencia de Tecnologías de la Información y Comunicaciones 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 Tecnologías de la Información y Comunicaciones 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.

4.15. Seguridad en la red - Uso de internet y de la red interna

a. El acceso a Internet está reservado para todos aquellos empleados, estudiantes, docentes de catedra y terceros que lo requieran según sus funciones.

b. 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.

c. En la red ADMINISTRATIVA se tiene navegación libre en los horarios de 12:00 pm a 2:00 pm y de 18:00 a 00:00.

d. Está prohibido para los empleados y terceros el acceso a red inalámbrica o cableada del Politécnico Grancolombiano, menoscabar o eludir los controles establecidos por la Institución para la protección de los activos de información.

e. 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 Tecnologías de la Información y Comunicaciones y por requisitos propios de la Institución.

f. Los sistemas de comunicación tales como modems, routers, switch, entre otros dispuestos por el Politécnico Grancolombiano, son los únicos autorizados para su uso en la red de la Institución.

g. Dentro de la red ADMINISTRATIVA se tiene prioridad al tráfico hacia OneDrive.

h. 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.

4.16. Conexiones Remotas

a. Toda conexión remota a la red de la Institución debe realizarse a través de canales seguros como VPNs o canales dedicados. Éstas deben solicitar autenticación para establecer la conexión remota a la red con el fin de prevenir accesos no autorizados.

b. El uso de la VPN 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 Grancolombiano 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 la VPN a quienes deban correr procesos en horarios no laborales, con previa autorización.

c. 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.

d. 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.

4.17. Seguridad en los desarrollos

a. 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.

b. El Director de Innovación y Desarrollo 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.

c. 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.

d. 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.

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 de la misma y se restaure en los ambientes de pruebas, sin difusión de la misma. Lo anterior con el fin de preservar la confidencialidad de la información, a efectos de no vulnerar las condiciones de seguridad de acuerdo con su clasificación.

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 del mismo.

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.

4.18. Seguridad para los proveedores, contratistas y terceros

a. 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.

b. 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.

c. 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.

d. 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 la misma y las penas a que estaría sujeto el Proveedor o Contratista en caso de incumplirlos. El cumplimiento de los acuerdos mencionados anteriormente debe ser verificado periódicamente por el Director de Seguridad y Activos de la Información y la Dirección Jurídica.

e. 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.

4.19. Administración de portales

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. Todos los portales deben exigir a los estudiantes cambiar la contraseña cada 120 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.

4.20. 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 Tecnologías de la Información y Comunicaciones.

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 Tecnologías de la Información y Comunicaciones 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.

4.21. Continuidad

a. La Gerencia de Tecnologías de la Información y Comunicaciones 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. El plan de continuidad de la Institución debe ser documentado, probado y evaluado por lo menos una vez al año, según el cronograma establecido por la Gerencia de Tecnologías de la Información y Comunicaciones para verificar su adecuado funcionamiento. Los horarios de prueba deben indicar que elemento del plan va a ser evaluado y con qué frecuencia.

c. Los planes de contingencia deben estar ubicados en un lugar seguro dentro del Politécnico Grancolombiano. Adicionalmente debe existir una copia en un sitio alterno con el fin de recuperar las operaciones de la Institución en caso de que la contingencia afecte las instalaciones. De igual forma, dicho plan debe ser de conocimiento de todos los empleados y distribuido según su inherencia a toda la estructura de la Institución.

4.22. Cumplimiento regulatorio

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

b. La Gerencia de Tecnologías de la Información y Comunicaciones 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. Todos los empleados están obligados a ceder al Politécnico Grancolombiano los derechos exclusivos de propiedad literaria, licencias, invenciones, u otra propiedad intelectual que ellos creen o desarrollen en desarrollo de las funciones asignadas durante su vinculación laboral con la Institución. En el caso de aplicaciones de terceros, este aspecto se rige por las condiciones y cláusulas establecidas en el contrato de adquisición de productos y servicios, con la finalidad de prevenir cualquier disputa respecto a la propiedad del software y licencias, una vez que el proyecto sea completado. Todo lo anterior se realiza de conformidad con lo establecido en la Política - Propiedad Intelectual y transferencia de conocimiento.

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 Tecnologías de la Información y Comunicaciones 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. La omisión por parte del personal involucrado en las obligaciones y responsabilidades definidas en esta política es considerada falta grave y, por ende, conlleva a la implementación de las medidas pertinentes por parte de la Institución.

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 el Área Jurídica y el Director de Seguridad y Activos de Información, con el fin de garantizar su aplicación adecuada y oportuna para la Institución.

k. El Área Jurídica es responsable de publicar y actualizar la normatividad con inherencia para la Seguridad de la Información.

l. El Director de Seguridad y Activos de Información, se comunicará con el Área Jurídica, cuando tenga conocimiento de una nueva legislación aplicable a cualquiera de los procesos de la Institución con respecto a seguridad de la información.

m. El Director de Seguridad y Activos de Información es el responsable de gestionar y hacer seguimiento a la implementación de las normas nacionales que apliquen a la seguridad de la información.

n. Todos los procesos y operaciones de la Institución deben regirse por la legislación colombiana vigente respecto a seguridad de la información.

4.23. Desarrollo Seguro

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.

4.23.1. 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.

4.23.2. Requerimientos específicos

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

- 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)

4.23.3. 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.

4.23.4. 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.

4.23.5. 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.
- 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.

4.23.6. 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.

4.23.7. 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.

- 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.

4.23.8. 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 del mismo 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.

4.23.9. Log / Auditoría

Asegurar que las aplicaciones bien escritas generen LOGS de doble propósito con trazas de actividad para auditoria 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.

4.23.10. 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.

4.23.11. 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.

- 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.

4.23.12. 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

4.23.13. 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).

Fase inicial y de desarrollo

a. Los analistas de servidores deberán revisar a solicitud de la Gerencia de Tecnologías de la Información y Comunicaciones y del Director de Seguridad y Activos de Información, los eventos de monitoreo ante cualquier tipo de caso de seguridad, generando un reporte de las evidencias encontradas e informando al Director de Seguridad y Activos de Información.

b. El Área de Redes y Servidores deberá evaluar cualquier tipo de evento/incidente de seguridad como Virus o Malware, con el fin de establecer soluciones que puedan ayudar a controlar cualquier tipo de eventualidad.

c. El Director de Seguridad y Activos de Información autoriza el bloqueo y/o suspensión temporal de la cuenta de correo electrónico corporativo y/o copia de cualquier tipo de correo que aún se encuentre en el servidor de correo, para que forme parte de un proceso de evidencia.
d. El Director de Seguridad y Activos de Información notifica la suspensión de la cuenta de correo electrónico del usuario.

e. El Director de Seguridad y Activos de Información solicitará la copia de respaldo del PST, a la Gerencia de Tecnologías de la Información y Comunicaciones.

f. El Director de Seguridad y Activos de Información, buscará evidencia en las copias de los PST y realizará un análisis forense siguiendo los procesos metodológicos y técnicas especializadas para este fin.

Fase final

El Director de Seguridad y Activos de Información realiza el "Informe Pericial" de resultados de las evidencias encontradas y los presenta a la Gerencia de Tecnologías de la Información y Comunicaciones, para determinar cuáles serán las acciones a seguir con el usuario comprometido en el evento de seguridad.

4.24. 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 las VPNs 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 Seguridad y Activos de Información 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 Seguridad y Activos de Información, 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 Seguridad y Activos de Información, 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 Seguridad y Activos de Información 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.

5. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DEL CAMBIO
V1	Lanzamiento del documento
V2	Actualización general de disposiciones
V3	Ajuste de plantilla, actualización de lineamientos.
V4	Actualización del encabezado y logo institucional. Cambios en el contenido del documento.