	MACROPROCESO	APOYO	CÓDIGO:	AGR-GT-PL-01
	PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN:	2
	POLÍTICA	SEGURIDAD DE LA INFORMACIÓN	PÁGINA:	i

DESCRIPCIÓN DEL PROCEDIMIENTO

OBJETIVO

Dar a conocer los lineamientos para garantizar altos niveles de integridad, disponibilidad y confidencialidad de la información que genera el Instituto Alexander von Humboldt (en adelante el "Instituto").

ALCANCE

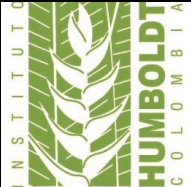
Esta política y todas las normas relacionadas con la seguridad de la información son de obligatorio cumplimiento para todos los trabajadores y contratistas del Instituto, así como para todos los externos que tengan acceso a la información física o electrónica que genera el Instituto.

NATURALEZA JURÍDICA DEL INSTITUTO

El Instituto es una corporación civil sin ánimo de lucro, sometida a las reglas del derecho privado, con autonomía administrativa, personería jurídica y patrimonio propio, vinculada al Ministerio del Ambiente y Desarrollo Sostenible (Minambiente), creada por la Ley 99 de 1993 con el encargo de realizar la investigación básica y aplicada sobre los recursos genéticos de flora y fauna nacionales, así como de levantar y formar el inventario científico de la biodiversidad en todo el territorio nacional.

LINEAMIENTOS GENERALES

- Es responsabilidad del Grupo de Tecnologías de la Información la elaboración, actualización, emisión, divulgación y verificación de la presente política.
- Para el diseño y construcción de esta política, se tuvieron en cuenta los lineamientos la Norma Técnica Colombiana NTC ISO/IEC 27001.
- Para la administración de la información, el Instituto deberá aplicar la ley 1581 de 2012 "Habeas Data"
- El Profesional Senior del Grupo de Tecnologías de la Información (TI) es responsable por la coordinación y orientación sobre la actualización permanente de la presente política. La actualización debe ser realizada en la medida en que ocurra alguno (o varios) de los siguientes eventos:
 1. Cambios en el ambiente de negocios o estrategia del Instituto (ejemplo: nuevas estrategias de investigación, cambio en las prioridades, fusiones o cesiones, cambios en la estructura organizacional, nuevas direcciones, etc.)
 2. Cambios en la infraestructura o de riesgos de seguridad de información del Instituto.
 3. Nuevas obligaciones legales y/o reglamentarias o cambio de las existentes que afecten el procesamiento de la información, intercambio de información con terceros, entre otros.
 4. Avances en las mejores prácticas de seguridad de la Información registradas en el código de prácticas ISO/IEC 27002 o cambios en la norma ISO/IEC 27001 y que previamente evaluadas sean necesarias para el Instituto.
 5. Aplicación de nuevos controles identificados como resultado de los análisis de los incidentes de seguridad de la información o el resultado de auditorías del Grupo de Tecnologías de la Información (TI).

	MACROPROCESO	APOYO	CÓDIGO:	AGR-GT-PL-01
	PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN:	2
	POLÍTICA	SEGURIDAD DE LA INFORMACIÓN	PÁGINA:	ii

DESARROLLO DE LA POLÍTICA

El Instituto teniendo en cuenta que la información y el conocimiento es un activo esencial para el normal desarrollo de las investigaciones, demás actividades misionales y procesos estratégicos y de apoyo del Instituto, define las normas que garanticen la integridad, disponibilidad y confidencialidad de la misma e invita a todas las partes interesadas (trabajadores, contratistas y proveedores) a acatarlas y velar por su cumplimiento, con el fin de garantizar altos estándares de seguridad a nuestra información y la de nuestros socios y clientes.

ORGANIZACIÓN DE SEGURIDAD

La Dirección General del Instituto se encargará de dar una dirección estratégica a la seguridad de la información acorde con los lineamientos del Instituto y aprobará las políticas, normas y procedimientos relacionados.

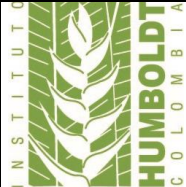
A continuación se describen las responsabilidades operativas de la seguridad de la información que deberá cumplir el Profesional Senior del Grupo de Tecnologías de la Información:

- Revisar y aprobar la política de seguridad de la información del Instituto.
- Revisar, evaluar, aprobar e implementar los controles de seguridad de la información.
- Identificar las tendencias y los cambios importantes de los riesgos de seguridad de la información del Instituto y proponer los cambios de políticas, normas y procedimientos adecuados con el fin de controlar las vulnerabilidades identificadas.
- Asegurar la divulgación de la política de seguridad de la información a todos los trabajadores.
- Establecer mecanismos de control que permitan medir el cumplimiento de las políticas, normas y procedimientos de seguridad de la información.
- Recomendar acciones correctivas a los incidentes de seguridad reportados.
- Hacer seguimiento a los incidentes de seguridad reportados.
- Establecer mecanismos de control de la información confidencial del Instituto.
- Realizar reportes periódicos a la Dirección del Instituto indicando el nivel de seguridad obtenido mediante la ejecución de los controles establecidos en la política de seguridad de la información.
- Desarrollar programas de concientización y capacitación a todos los trabajadores que enfatice la importancia del cumplimiento de la política de seguridad de la información y su contribución al logro de los objetivos del Instituto.
- Entregar informe de eventos cuando ocurra un incidente de seguridad que requiera un seguimiento y atención especial o por la declaratoria de contingencia técnica y/o operativa.

NORMAS DE GESTIÓN Y ADMINISTRACIÓN DE ACTIVOS DE INFORMACIÓN

Inventario de los activos de información

- Cada uno de los trabajadores del Instituto debe entregar los datos (información) almacenados en los equipos de cómputo y/o bases de datos de los servidores, necesarios para el desarrollo de las actividades al momento de su retiro definitivo, lo anterior para poder realizar una copia de seguridad sobre esta información.
- La información será almacenada y custodiada por personal del Grupo de Tecnologías de la Información quienes serán los responsables de mantener esta información disponible y será tratada conforme el procedimiento *AGR-GT-P-08 Gestión y Control de Backups*.

	MACROPROCESO	APOYO	CÓDIGO:	AGR-GT-PL-01
	PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN:	2
	POLÍTICA	SEGURIDAD DE LA INFORMACIÓN	PÁGINA:	iii

DESARROLLO DE LA POLÍTICA

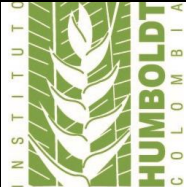
- Los datos y/o activos de información (Backpus) cuando se encuentre en el data center y en medida en que el responsable de la información lo requiera y el Grupo de Tecnologías de Información lo apruebe, se realizara un backup según la frecuencia definida por T.I.
 - a. Full backup conforme periodicidad definida.
 - b. Full backup e incremental conforme periodicidad definida.
- El Grupo de Tecnologías de la Información es el encargado de realizar el inventario de los aplicativos y programas bajo licencia con que cuenta el Instituto. Los datos que debe incluir el inventario son:
 - a. Nombre del aplicativo o software
 - b. Versión
 - c. En donde está instalada cada licencia y un control de las claves de instalación de las mismas.
- En el Grupo de Tecnologías de la Información deben gestionar las hojas de vida de los activos del parque tecnológico del Instituto donde se identifique la información de hardware y software instalado, asignación y re asignaciones a trabajadores.
- La hoja de vida de los activos del parque tecnológico debe ser actualizado en la medida en que ocurra uno o varios cambios:
 - a. Cambios en el ambiente de servicios o estrategia del Instituto.
 - b. Renovación o actualización tecnológica.
 - c. Desarrollo o compra de un sistema de información (aplicativo)
 - d. Pasado un año de la última actualización del inventario.

Responsabilidad de los activos de información

- **Los** propietarios o responsables de los activos de información deben ser claramente designados por la Dirección del Instituto. Los propietarios serán los responsables de la protección de los activos de información contra incidentes de seguridad.
- Los propietarios de los activos de información, son responsables por la clasificación de sus activos y la definición y auditoria constante de las restricciones de acceso y otros controles de seguridad de la información.

Clasificación de la información

- Los responsables de la información en medio magnético deben realizar la clasificación de acuerdo a los criterios de confidencialidad, sensibilidad, riesgo de pérdida o compromiso, aspectos legales, requerimientos de retención y facilidad de recuperación que deben ser empleados.
- Los requerimientos legales, estatutarios y regulatorios deben ser considerados al momento de evaluar la clasificación de la información.
- La clasificación de la información debe ser realizada simultáneamente con el inventario.
- Los criterios para clasificar la información son:

	MACROPROCESO	APOYO	CÓDIGO:	AGR-GT-PL-01
	PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN:	2
	POLÍTICA	SEGURIDAD DE LA INFORMACIÓN	PÁGINA:	iv

DESARROLLO DE LA POLÍTICA

a. Información de uso público o informativo.

Su divulgación no requiere de autorización especial dentro y fuera del Instituto y su función es de comunicación del personal en general.

Puede darse a conocer al público en general a través de carteleras, Intranet, comunicaciones oficiales, entre otros.

b. Información de uso interno o privada

Su divulgación no autorizada, principalmente fuera del Instituto sería inadecuada o inconveniente, debe ser de conocimiento únicamente por parte de los trabajadores del Instituto.

Puede ser compartida entre áreas dada su necesidad para la operación diaria y no consolida resultados finales de gestión.

c. Información de uso confidencial

Sustenta estrategias de investigación del Instituto, información financiera consolidada, informes de gestión para la Junta Directiva y Dirección, registros para toma de decisiones, información de clientes y competencia, información de personal y cualquier otra que pueda comprometer la seguridad del Instituto o de las personas.

Su divulgación no está autorizada, incluso dentro del Instituto.

- La información de los socios, clientes, investigadores, trabajadores es confidencial en todo el Instituto.

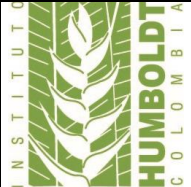
Controles para el manejo la información clasificada como confidencial

- El envío a un tercero de información clasificada como confidencial debe ser autorizado por el responsable de la información y/o el Director General del Instituto.
- La información clasificada como confidencial que sea necesario entregar a un tercero, debe ser entregada utilizando mecanismos definidos por el Grupo de Tecnologías de la Información (TI) para que se garanticen su confidencialidad.
- El acceso a la información confidencial almacenada en las bases de datos y archivos digitales debe ser estrictamente controlado.

NORMAS DE SEGURIDAD DEL PERSONAL

Cumplimiento de las políticas y normas de Seguridad de la información

- Es obligación de los usuarios, sin excepción alguna, conocer, respetar, cumplir y hacer cumplir la política de seguridad de la información del Instituto.

	MACROPROCESO	APOYO	CÓDIGO:	AGR-GT-PL-01
	PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN:	2
	POLÍTICA	SEGURIDAD DE LA INFORMACIÓN	PÁGINA:	v

DESARROLLO DE LA POLÍTICA

Acuerdos de confidencialidad

- Todos los trabajadores y contratistas que manejen información o datos de y para el Instituto, suscribirán acuerdos de confidencialidad o se incluirá en sus contratos una cláusula de confidencialidad, sin perjuicio de lo previsto en el Reglamento interno de trabajo del Instituto.

Procesos disciplinarios

- Todo fallo de seguridad presuntamente cometido por un trabajador del Instituto será objeto de investigación establecida en el Reglamento Interno de Trabajo y las sanciones consecuentes.
- Si el incidente afecta económicamente o la reputación del Instituto, se iniciarán las acciones civiles correspondientes de acuerdo a la legislación vigente.

Terminación o cambio de empleo de los trabajadores

- Todos los trabajadores que se retire del Instituto, debe hacer entrega al jefe de área, al Grupo Gestión Logística y Documental y al Grupo de Tecnologías de la Información (TI), de los activos informáticos asignados para su cargo (incluyendo documentos, archivos digitalizados, computadores, dispositivos externos de almacenamiento, tarjeta de acceso, información de terceros almacenada en teléfonos móviles o portátiles y las contraseñas de los diferentes usuarios en los sistemas de información).
- El acceso a la información, computadores, redes de datos e instalaciones físicas, deben ser revocadas de inmediato cuando un trabajador o un tercero se retira del Instituto.

NORMAS DE SEGURIDAD FISICA

Áreas de acceso restringido

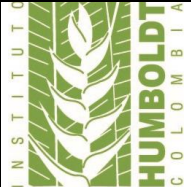
Se definen como aquellas áreas que necesitan autorización previa para permitir el ingreso de personas ajenas al área, por la naturaleza de la información confidencial o sensible que se maneja o los procesos que allí se realizan. Dentro del Instituto, se identificaron las siguientes áreas de acceso restringido:

- a. Centro de Procesamiento de Datos CDP (Datacenter).
- b. Área de Grupo Administración Recursos Financieros.
- c. Centros de cableado estructurado y servidores.

Una vez autorizado el ingreso del visitante, el trabajador visitado deberá recogerlo y acompañarlo todo el tiempo durante el recorrido o su permanencia en el área segura.

Control de acceso a áreas seguras

- Las personas autorizadas para ingresar y permanecer en el área son los trabajadores y los terceros autorizados de la misma.
- La autorización del acceso de visitantes a las áreas seguras está en cabeza de Jefe del Área o el delegado de ésta de acuerdo al procedimiento establecido según corresponda.
- Registrar el ingreso al Centro de Procesamiento de Datos CDP (Data center) en la bitácora definida para

	MACROPROCESO	APOYO	CÓDIGO:	AGR-GT-PL-01
	PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN:	2
	POLÍTICA	SEGURIDAD DE LA INFORMACIÓN	PÁGINA:	vi

DESARROLLO DE LA POLÍTICA

este caso.

Protección y ubicación de equipos tecnológicos

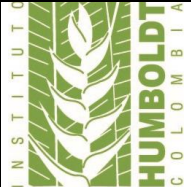
- Todos los equipos principales que soportan los aplicativos, bases de datos, sistemas de comunicación y sistemas de seguridad se deben alojar en áreas restringidas protegidas por un perímetro de seguridad y con controles de acceso físico.
- Está totalmente prohibido retirar computadores o algunos de sus accesorios fuera de las instalaciones del Instituto sin la debida autorización del Grupo Gestión Logística y Documental.
- El retiro o traslado de cualquier equipo de cómputo del Instituto debe contar con una justificación la cual será autorizada por el Grupo Gestión Logística y Documental y el movimiento físico deberá ser comunicado al Grupo de Tecnologías de la Información (TI), ver procedimiento *AGR-LD-P-03 Ingreso, novedades y salidas de bienes*.
- Está prohibido manipular las redes de cableado estructurado de voz, datos o eléctrico, así como instalar cables, extensiones eléctricas y dispositivos tecnológicos que no sean propiedad del Instituto sin previa autorización Grupo de Tecnologías de la Información (TI)

Protección de centro procesamiento de datos (Data center)

- El centro de procesamiento de datos del Instituto, debe incorporar medidas de protección para reducir al mínimo la posibilidad y las repercusiones de incidentes como incendios, inundaciones, terremotos, explosiones, disturbios civiles, que su consecuencia sea la pérdida de la información.
- El sistema eléctrico del centro de procesamiento de datos debe contar con un sistema de UPS, así como de condiciones eléctricas acordes a las normas internacionales.
- Los operadores, administradores y terceros frecuentes al centro de procesamiento de datos, deben ser capacitados en los procedimientos que deben seguir cuando se presente un evento de origen físico que afecte la continuidad en la operación normal del centro de cómputo.
- Para todos los visitantes al centro de procesamiento de datos, se registrará la fecha y hora de ingreso, motivo de la visita y fecha y hora de la salida. Esta información se registra en la bitácora de visitas al centro de procesamiento de datos. Esta bitácora debe estar disponible por un periodo de tiempo no inferior a un año.
- Se debe establecer y ejecutar un plan de mantenimientos preventivos que cubija todos los recursos informáticos y de soporte ambiental del centro de cómputo.
- Está totalmente prohibido fumar y consumir alimentos en el centro de procesamiento de datos.

Política de Equipos desatendidos:

Cuando un trabajador se retire temporalmente de su puesto de trabajo, debe hacer un logout de la sesión del aplicativo y activar el bloqueo del escritorio de trabajo del computador mediante la opción de protector de pantalla o que el sistema operativo bloquee el escritorio después de 10 minutos de inactividad.

	MACROPROCESO	APOYO	CÓDIGO:	AGR-GT-PL-01
	PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN:	2
	POLÍTICA	SEGURIDAD DE LA INFORMACIÓN	PÁGINA:	vii

DESARROLLO DE LA POLÍTICA

NORMAS DE SEGURIDAD EN LA ADMINISTRACIÓN DE OPERACIONES DE TECNOLOGÍA

Normas de control de cambios a servidores y equipos de infraestructura

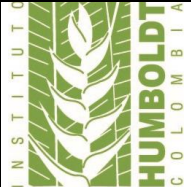
- Está totalmente prohibida la instalación de servidores sin la autorización del Grupo de Tecnologías de la Información (TI)
- Los cambios de configuración de los servidores deben ser realizados por personal del Grupo de Tecnologías de la Información (TI) exclusivamente.
- Antes de realizar un cambio crítico en la configuración de los servidores, se debe realizar un backup a la información almacenada y a la configuración del sistema.
- Los cambios realizados a los servidores, a cargo de los administradores del Instituto deben ser registrados en la bitácora de cambios definida desde el Grupo de Tecnologías de la Información (TI)
- Los parches de actualización se deben aplicar de acuerdo a la siguiente programación:
 - a. Los parches de seguridad o catalogados como urgentes y críticos, se deben aplicar de manera automática una vez son liberados por la casa fabricante del sistema operativo.
 - b. Los parches de actualización para los servidores deben ser revisados y aplicados según las necesidades siguiendo el procedimiento de actualización de parches de sistema operativo con una periodicidad no mayor a un año.

Políticas de renovación tecnológica

- El hardware del parque tecnológico del Instituto clasificados de misión crítica, debe ser actualizado o renovado de acuerdo con el plan de renovación que se definida.
- El software y hardware instalado del parque tecnológico del Instituto, debe estar soportado por proveedores locales o extranjeros autorizados por el fabricante. Una vez la casa fabricante del software y hardware anuncie la finalización del soporte sobre la versión del software o hardware instalado, este debe ser actualizado a la versión más reciente.

Normas de control de código malicioso

- El Grupo de Tecnologías de la Información debe garantizar que todos los computadores conectados en la red del Instituto tengan instalado el software antivirus.
- El Grupo de Tecnologías de la Información debe implantar los mecanismos de actualización permanente y en línea del software antivirus instalado en los computadores conectados en la Red. De igual forma, se debe garantizar un mecanismo semiautomático o manual que permita la actualización del antivirus instalado en computadores que no se conectan de manera permanente a la red.
- Periódicamente se debe revisar la consola de administración del software antivirus, con el fin de identificar los computadores que no tienen la última versión instalada. De ser necesario, se aplicará un procedimiento manual de actualización por parte del Grupo de Tecnologías de la Información.

	MACROPROCESO	APOYO	CÓDIGO:	AGR-GT-PL-01
	PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN:	2
	POLÍTICA	SEGURIDAD DE LA INFORMACIÓN	PÁGINA:	viii

DESARROLLO DE LA POLÍTICA

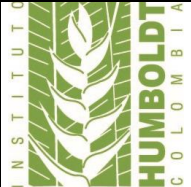
- El software antivirus debe ser configurado para el escaneo en línea de todas las unidades de almacenamiento.
- Todo CD, DVD, memoria USB, disco duro externo que sea conectado en un computador del Instituto independientemente de su procedencia, debe ser escaneado con el software antivirus de forma automática antes de ser utilizado.
- Los usuarios deben reportar de inmediato al Grupo de Tecnologías de la Información (TI) el comportamiento anormal del computador o indicio de la presencia de virus, con el fin de prevenir la propagación del mismo.
- Ante la presencia de un virus, se debe atender el caso desde el Grupo de Tecnologías de la Información, para revisar el equipo y garantizar la eliminación del virus sin que este afecte otros equipos en la red.

Normas de Backup de información crítica

- Los requerimientos que se deben tener en cuenta en la estrategia de respaldo de crítica para los objetivos del Instituto almacenada en cada uno de los servidor son:
 - a. Identificación de la Información crítica a la que se debe realizar copia de seguridad.
 - b. Nivel de confidencialidad de la información respaldada.
 - c. Periodicidad de la generación de copias de seguridad.
 - d. Periodo retención, acceso y disponibilidad en centro de procesamiento de datos.
- Es responsabilidad del Grupo de Tecnologías de la Información el respaldo, control y manejo del software de backup, el cual es utilizado para realizar las copias de la información crítica almacenada en cada uno de los servidores.
- Es responsabilidad del Grupo de Tecnologías de la Información la supervisión periódica de los procesos de toma de backup, rotación, custodia y almacenamiento de las cintas de backup.
- Las cintas de backup de la información crítica del Instituto se deben almacenar en un sitio externo (fuera de las instalaciones del Centro de Procesamiento de Datos) con controles de acceso restringido y con las condiciones ambientales adecuadas.
- Periódicamente, se deben realizar pruebas de restauración de una cinta de backup de un servidor de red.

Normas para el monitoreo de recursos de TI

- Los registros de auditoria que reporten las fallas de aplicativos, servidores, sistemas operativos, bases de datos, sistemas de protección perimetral y sistemas de control ambiental deben ser revisadas periódicamente y de manera preventiva y tomar las medidas adecuadas para detectar y prevenir posibles incidentes que afecten la continuidad de los procesos del Instituto.
- Los perfiles de administrador sobre las sesiones de red, solo son utilizados por el personal del Grupo de Tecnologías de la Información del Instituto.

	MACROPROCESO	APOYO	CÓDIGO:	AGR-GT-PL-01
	PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN:	2
	POLÍTICA	SEGURIDAD DE LA INFORMACIÓN	PÁGINA:	ix

DESARROLLO DE LA POLÍTICA

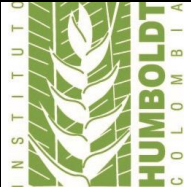
NORMAS DE CONTROL DE ACCESO LÓGICO A LOS APLICATIVOS DEL INSTITUTO

Política de control de acceso lógico

- Todos los recursos informáticos y/o aplicativos del Instituto deben usar controles de acceso lógico, con el fin de prevenir el acceso no autorizado a la información confidencial o sensible.
- El control de acceso a la información debe ser definido, aprobado y documentado por los responsables de la información y deben estar basados en requerimientos específicos del Instituto.
- Se deben crear perfiles de acceso asociados a roles que tienen responsabilidades y cumplen con actividades comunes (cargos); estos perfiles deben permitir el acceso mínimo y suficiente para el adecuado desempeño de las actividades de los usuarios.
- Los permisos de acceso a las redes, servicios y sistemas de información del Instituto, serán otorgados mediante un proceso de aprobación que asegure el tener acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.
- Todos los trabajadores y personal externo que accede a los sistemas de información deben tener un usuario del directorio activo y sus credenciales son personales e intransferibles, con lo cual será responsable de mantener su confidencialidad y asegurar su correcto uso.
- Se deben deshabilitar o actualizar los privilegios de acceso a los recursos informáticos inmediatamente se presente la novedad correspondiente o cuando se genere un cambio de privilegios en un rol o perfil.
- Cuando un trabajador o un usuario externo deja el Instituto, o cambia de cargo, se deben eliminar o reasignar sus privilegios de acceso a los recursos informáticos del Instituto.
- Los aplicativos deben ser el único mecanismo para acceder los datos e información del Instituto.

Registro de usuarios

- A cada usuario del Instituto que requiera acceso a los sistemas de información, se le asignará un único código de usuario, el cual es de carácter personal e intransferible.
- La creación, modificación y eliminación de cuentas de usuarios debe ser realizada mediante un procedimiento formal y debe ser autorizado por el responsable de los datos.
- El responsable de la información deberá comunicar al Grupo de Tecnologías de la Información si se debe deshabilitar los códigos de usuario que no requieren el acceso a los sistemas de información por un periodo de tiempo determinado. Ejemplo funcionarios que salen de vacaciones, licencias, etc. Está totalmente prohibido que las áreas utilicen los códigos de usuarios de funcionarios que se encuentren ausentes del Instituto.
- Los usuarios que presenten cinco (5) intentos fallidos en el momento de digitar la contraseña deben ser bloqueados por los sistemas de información y solicitar su acceso al Grupo de Tecnología de la Información, esto con el fin de validar que esta persona si cuenta con el acceso.

	MACROPROCESO	APOYO	CÓDIGO:	AGR-GT-PL-01
	PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN:	2
	POLÍTICA	SEGURIDAD DE LA INFORMACIÓN	PÁGINA:	x

DESARROLLO DE LA POLÍTICA

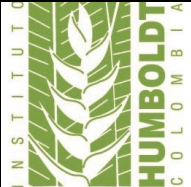
- La eliminación de accesos y servicios de red asociados a un código de usuario debe ser realizada inmediatamente el trabajador ha finalizado su vinculación laboral/contractual con el Instituto o ha cambiado de cargo dentro del Instituto y no se requiere que acceda a éstos recursos informáticos.

Política de administración de contraseñas para Directorio Activo.

- Las contraseñas deben cumplir con el siguiente estándar:
 - a. Longitud mínima de 8 caracteres.
 - b. Alfanumérica.
- La contraseña expira cada 60 días y debe ser cambiada por los trabajadores. El sistema avisara 8 días antes que se debe cambiar la contraseña.
- El sistema debe solicitar el cambio de la contraseña de manera obligatoria la primera vez que se ingrese al sistema.
- El cambio de contraseña por bloqueo de usuario es obligatorio para el siguiente ingreso.

Política de uso del correo electrónico

- El servicio de correo electrónico del Instituto es para uso exclusivo de las actividades relacionadas con el trabajo de cada empleado.
- Se prohíbe la difusión no solicitada de puntos de vista personales que afecten o puedan afectar derechos de terceros, al igual que usar el email para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular.
- Se prohíbe fomentar el envío de cadenas de mensajes, recepción o envío de mensajes con fines ajenos a la misión institucional, cualquiera que sea su formato.
- Este servicio no debe usarse para enviar SPAM o mensajes no solicitados ni tampoco para enviar material obsceno e ilegal o relacionado a pornografía infantil.
- Está prohibido configurar reglas en los buzones de correo electrónico que reenvíen los mensajes a servidores públicos u otros correos electrónicos personales de internet.
- No se puede utilizar el correo electrónico, para intimidar, insultar o acosar a otras personas, interferir con el trabajo de los demás provocando un ambiente de trabajo no deseable dentro del contexto de las políticas del Instituto.
- No se puede usar para la transmisión, distribución, almacenamiento de cualquier material protegido por las leyes vigentes. Esto incluye sin limitación alguna, todo material protegido por derechos de autor (copyright), Marcas registradas, secretos comerciales u otros de propiedad intelectual.
- El tamaño de los archivos adjuntos no debe exceder de 20 MB, este tamaño puede ser chequeado por medio de las propiedades de cada archivo. Si el archivo adjunto excede este tamaño, es necesario comprimir el archivo.

	MACROPROCESO	APOYO	CÓDIGO:	AGR-GT-PL-01
	PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN:	2
	POLÍTICA	SEGURIDAD DE LA INFORMACIÓN	PÁGINA:	xi

DESARROLLO DE LA POLÍTICA

- En caso de recibir un mensaje bajo sospecha de virus, (de personas desconocidas con asuntos desconocidos o sospechosos) no se debe abrir y se debe marcar como correo NO deseado y reportar de inmediato el incidente al Grupo de Tecnologías de la Información (TI)

Políticas de uso de Internet

- El acceso a internet debe ser con el fin de desarrollar actividades institucionales.
- El acceso a internet NO puede ser utilizado para los siguientes propósitos:
 - Actividades relacionadas a juegos online por internet
 - Ingreso a cualquier material que viole de manera evidente el derecho de terceros y que no guarde relación con la actividad institucional o viole el Reglamento Interno de Trabajo.
 - Ingreso o fomento de páginas de pornografía infantil
 - Utilizar servicios de descarga de archivos P2P.
 - Servicios de Streaming, webcast, y/o videoconferencias no correspondientes al desarrollo de sus funciones.
 - Utilizar los servicios de Internet para enviar archivos que sean confidenciales y de propiedad exclusiva del Instituto.
 - Cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocios particulares.
 - Utilizar los servicios de internet para la transmisión, distribución o almacenamiento de cualquier archivo protegido por las leyes vigentes. Esto incluye todos los archivos protegidos por derechos de autor, marcas registradas, secretos comerciales u otros de propiedad intelectual.

NORMAS DE ADQUISICIÓN Y MANTENIMIENTO DE APLICATIVOS

Software estándar para equipos de computo

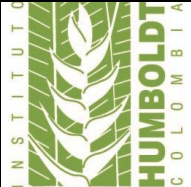
- El software estándar que debe ser instalado a todos los equipos de cómputo del Instituto será definido por el Grupo de Tecnologías de la Información (TI)

Software estándar para servidores

- El software estándar que debe ser instalado a todos los servidores del Instituto será definido por el Grupo de Tecnologías de la Información (TI)

Políticas de instalación y uso de software

- El software estándar de equipos de cómputo y servidores, así como el software autorizado que no hace parte del estándar, solo será instalado y autorizado por personal del Grupo de Tecnologías de la Información del Instituto.
- Toda adquisición de software nuevo que sea necesario para el soporte de actividades de las diferentes áreas debe ser adquirido a través del Grupo de Tecnologías de la Información (TI).
- Desde el Grupo de Tecnologías de la Información se administrarán todas las licencias de software, así como los medios magnéticos de instalación y configuración. Ningún funcionario del Instituto está autorizado para

	MACROPROCESO	APOYO	CÓDIGO:	AGR-GT-PL-01
	PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN:	2
	POLÍTICA	SEGURIDAD DE LA INFORMACIÓN	PÁGINA:	xii

DESARROLLO DE LA POLÍTICA

adquirir o instalar software sin la aprobación del Grupo de Tecnologías de la Información (TI).

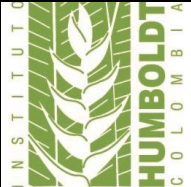
- Desde el Grupo de Tecnologías de las Información del Instituto se implementarán los controles necesarios para realizar un inventario de software y podrá desinstalar cualquier software no autorizado sin previo aviso. Adicionalmente, se debe tener un reporte de los usuarios que tienen instalado software no autorizado con el fin de que se tomen las medidas correctivas definidas por el Instituto.
- El software estándar instalado debe ser renovado una vez sea amortizado totalmente o el fabricante del mismo suspenda el soporte de la versión instalada previo análisis del Grupo de Tecnologías de la Información (TI)

Política de control de cambios para el desarrollo de software

- El desarrollo del software debe ser realizado bajo ambientes físicos y lógicamente separados.

Los ambientes deben ser:

- Ambiente de desarrollo con control de acceso para los analistas de desarrollo de software interno y/o externos.
 - Ambiente de pre-producción o pruebas el cual debe tener control de acceso restringido a los analistas de desarrollo de software.
 - Producción con bloqueo total para los analistas de desarrollo.
- El desarrollo de aplicativos debe ser realizado exclusivamente en los ambientes definidos para este propósito, estos ambientes o servidores que pueden ser del Instituto o de sus proveedores externos.
 - El ambiente de desarrollo preferiblemente debe tener datos ficticios para las pruebas de los analistas de desarrollo.
 - Las pruebas de usuario deben ser realizadas en el ambiente de pruebas con datos similares a los de producción.
 - El paso de programas desarrollados a los ambientes de producción, debe ser autorizado por los líderes del proceso una vez sean aprobadas las pruebas de operatividad del software desarrollado.
 - Por parte del analista desarrollador se debe entregar las últimas tres versiones de los aplicativos instalados en producción al Grupo de Tecnologías de la Información del Instituto.
 - La instalación de un aplicativo nuevo, así como las actualizaciones de los aplicativos en producción, deben ser acompañadas por la documentación técnica, operativa y de usuario correspondiente. No se autorizara la instalación de nuevos aplicativos o actualizaciones que no cuenten con la documentación completa. La documentación técnica de los aplicativos debe contener el DRP (plan de recuperación de desastres) de cada uno de ellos con los procedimientos de instalación, configuración y parametrización.
 - Cada área que cuente con analistas desarrollador deberá ser responsable por cumplir la política de control de cambios para el desarrollo de software del Grupo de Tecnologías de la Información (TI)

	MACROPROCESO	APOYO	CÓDIGO:	AGR-GT-PL-01
	PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN:	2
	POLÍTICA	SEGURIDAD DE LA INFORMACIÓN	PÁGINA:	xiii

DESARROLLO DE LA POLÍTICA

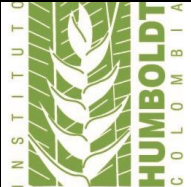
CAPACITACION DE USUARIOS DE TI

En caso de requerirse capacitación o formación en nuevas tendencias o mejores prácticas de temas relacionados con tecnologías de la información o seguridad informática y estas tengan un costo, el profesional Senior del Grupo de Tecnologías de la Información enviará solicitud formal al Grupo de Gestión Humana con autorización previa del Subdirector financiero y Administrativo.

Las capacitaciones son de obligatorio cumplimiento para los trabajadores que se definan desde el Grupo de Tecnologías de la Información (TI)

NORMAS DE CONTINUIDAD DEL NEGOCIO

- El Instituto debe diseñar, implementar, operar, probar y mantener un plan de continuidad para los procesos críticos del negocio.
- El Plan de continuidad del negocio, debe ser aprobado por el comité directivo del Instituto.
- El Instituto debe garantizar la disponibilidad de los recursos humanos, técnicos y financieros necesarios para la implementación y operación del Plan de continuidad.
- Dentro del plan de continuidad de negocio se debe realizar una evaluación formal de riesgo y análisis del impacto sobre las actividades que realiza el Instituto (BIA - Business Impact Assessment), con el fin de determinar los requerimientos del Plan de Continuidad del Negocio e identificar eventos que puedan causar interrupciones a los procesos tecnológicos del Instituto. Es importante considerar que se deben evaluar y analizar todos los procesos críticos y no limitarse exclusivamente a los recursos e infraestructura asociado a los sistemas de información.
- Con el fin de garantizar su consistencia a lo largo de las diferentes unidades de negocio, el plan de continuidad de negocio debe considerar los siguientes factores:
 - a. Condiciones para su activación.
 - b. Una estrategia de recuperación de desastres teniendo en cuenta aspectos como:
 - i. Costos de las diferentes alternativas.
 - ii. Costos de servicios alternos.
 - iii. Prioridades y tiempos de recuperación.
 - iv. Usuarios internos y externos, servicios, aspectos técnicos e información afectada.
 - c. Identificación de las responsabilidades.
 - d. Documentación de procedimientos y procesos acordados.
 - e. Educación apropiada sobre manejo de riesgos.
 - f. Cronograma de pruebas del plan de continuidad del negocio.
 - g. Responsabilidades individuales de ejecución y propietarios de cada plan.
 - h. El compromiso por parte de todas las personas involucradas en las actividades del plan, puesto que son el eje principal de la organización.
- Todos los trabajadores del Instituto deben conocer el Plan de Continuidad del Negocio y sus responsabilidades dentro de él.
- Se deben hacer talleres de sensibilización sobre el Plan de Continuidad del Instituto para su entendimiento y

	MACROPROCESO	APOYO	CÓDIGO:	AGR-GT-PL-01
	PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN:	2
	POLÍTICA	SEGURIDAD DE LA INFORMACIÓN	PÁGINA:	xiv

DESARROLLO DE LA POLÍTICA

conocimiento de responsabilidades por todos los trabajadores del Instituto.

- El Plan de Continuidad del Instituto necesita ser revisado y actualizado periódicamente, con el fin de que sea vigente para el Instituto.
- Al Plan de Continuidad del Instituto, se le deberán realizar simulaciones que permitan evaluar su viabilidad.
- En caso de que ocurra alguno de estos cambios, se deberá actualizar el Plan de Continuidad del Instituto:
 - a. Adquisiciones de nuevos equipos de la infraestructura primaria del Instituto.
 - b. Actualizaciones en los sistemas información primarios del Instituto.
 - c. Cambio en las Políticas de tecnologías de la información definidas por el Instituto.
 - d. Ubicaciones físicas.
 - e. Normas y regulaciones.
 - f. Procesos nuevos o eliminados.
 - g. Disposición de recursos humanos y financieros.

NORMAS DE CUMPLIMIENTO DE LOS REQUISITOS LEGALES

Derechos de propiedad intelectual

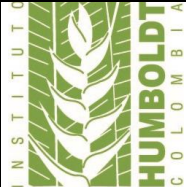
- Está prohibido el almacenamiento y uso de archivos con extensiones .avi, .mp3, .mpg, .Jpg los cuales corresponden a archivos de video, música, gráficos, juegos, entre otros. Que no estén debidamente licenciados por el Instituto o que no contribuyan a la misión Institucional.
- La instalación de software en los computadores del Instituto debe ser previamente autorizada por GTI y debe cumplir con los requerimientos legales que faculden su utilización.
- El software que reside en los computadores del Instituto sólo podrá ser el autorizado por el Profesional Senior de Tecnologías de la Información (TI). No se podrá instalar en los computadores del Instituto software que no esté registrado y autorizado.
- Desde el Grupo de Tecnologías de la Información se realizarán revisiones periódicas al software instalado en los equipos de cómputo y se eliminarán sin previo aviso todos los aplicativos y archivos que no estén autorizados previamente

Propiedad intelectual

- Todos los desarrollos de software realizados por funcionarios del Instituto, contratados o producidos bajo acuerdos que le asignen la propiedad intelectual del trabajo al Instituto son de propiedad del Instituto.

Cumplimiento de políticas de seguridad de la información

- La violación deliberada de las políticas de seguridad de la información y el incumplimiento de regulaciones, será sancionada mediante un proceso disciplinario ejecutado por el Grupo de Gestión Humana para el caso de funcionarios de Las Empresas o a través de contratos o procesos jurídicos en caso de terceros.

	MACROPROCESO	APOYO	CÓDIGO:	AGR-GT-PL-01
	PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN:	2
	POLÍTICA	SEGURIDAD DE LA INFORMACIÓN	PÁGINA:	xv

HISTORIAL DE CAMBIOS			
VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	AUTOR DEL CAMBIO
0	Enero, 2015	En la documentación del procedimiento se incorporó su diagrama de flujo, se realizaron ajustes a algunas actividades del procedimiento y se actualizo a la versión más reciente	Grupo de Tecnologías de la Información
1	Agosto 2016	Se realizan ajustes a las actividades descritas en el documento y se actualiza a la versión más reciente	Grupo de Tecnologías de la Información
2	Agosto 2020	Se realizan ajustes de actividades relacionadas al Grupo de Tecnologías de la Información	Grupo de Tecnologías de la Información

Elaborado Edwin Ríos	por:	Cargo: Profesional Senior Grupo de Tecnologías de la Información	Firma:	Fecha: Julio 2020
Revisado Marcelo Betancur	por:	Cargo: Subdirector Financiero y Administrativo	Firma:	Fecha: Agosto 2020
Aprobado Comité Directivo Sistema Integrado de Gestión MECI-SGC	por:		Acta:	Fecha: