Política Seguridad de la Información TI-002

Lineamientos Seguridad de la Información.

Índice

1. Introducción

La información es el activo más preciado de las empresas y entidades en general, por tanto se deben tomar todas las precauciones necesarias, para mantener y preservar información, para ello el Instituto Distrital de Ciencia, Biotecnología e Innovación en salud (IDCBIS), implementa un modelo de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes, esto soportado en tres pilares fundamentales confidencialidad, integridad y disponibilidad; así como adoptando buenas prácticas en cuanto a la gestión y administración de las Tecnologías de la Información.

Por lo anterior, con este documento se busca establecer lineamientos con relación a la seguridad de la información del Instituto Distrital de Ciencia, Biotecnología e Innovación en salud (IDCBIS), describiendo lo que se espera de todo el personal que trabaja para el IDCBIS y para todos aquellos que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información o recursos tecnológicos de la entidad en general. La Política de Seguridad refleja requerimientos de orden legal, ético y de mejores prácticas en el ejercicio de las actividades que se ejecutan a diario. Las medidas que se implementan no sólo son soluciones técnicas, sino también reflejan reglas claramente definidas, para dar el mejor uso a los recursos de TIC, por parte del usuario final de la plataforma tecnológica de la SDS.

2. Objetivo General

Establecer lineamientos de seguridad de la información para los colaboradores y visitantes del Instituto Distrital de Ciencia, Biotecnología e Innovación en salud (IDCBIS), que permitan el uso y protección adecuada de los recursos de información y de las comunicaciones.

3. Objetivos Específicos

- Evitar que los datos estén libres de modificaciones no autorizadas “Integridad”.
- Permitir que la información sea accesible sólo para aquellos usuarios autorizados a tener acceso “Confidencialidad”.
- Permitir el acceso a la información y a los sistemas a los usuarios autorizados en el momento que así lo requieran “Disponibilidad”.

4. Alcance

Las políticas definidas en este documento son de aplicación para todo el personal que tiene vinculo dentro Instituto Distrital de Ciencia Biotecnología e Innovación en Salud (IDCBIS).

5. Responsables.

La supervisión del cumplimiento de los "Lineamientos Seguridad de la Información", queda a cargo del Grupo de IT; razón por la cual está facultada para verificar en cualquier momento el cumplimiento de estos lineamientos y de las normativas vigentes en materias de tecnologías de información y comunicación.

Los **propietarios de activos de información** (ver su definición en definiciones) son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

La información que reside en cada PC o medio de almacenamiento auxiliar (CD, USB, Disco externo etc.) es responsabilidad de cada usuario.

El grupo de **Innovación y Desarrollo** cumplirá la función de notificar a todo el personal que se vincula contractualmente con el instituto, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal.

El grupo TI, es el único autorizado para ingresar a la red del instituto, nuevos recursos y sistemas informáticos (Software, hardware, seguridad, equipos de red etc.). TI será el responsable de coordinar el mantenimiento preventivo y correctivo de equipos; las reparaciones y/o ampliaciones de los mismos no pueden ser realizadas o contratadas por colaboradores que no hagan parte del grupo de TI.

Todo el personal del IDCBIS (funcionarios y contratistas) serán responsables civil y penalmente, por la mala utilización de la información reservada.

El uso o conexión a los recursos y servicios de TI del IDCBIS, implica el total conocimiento y aceptación de las normas y políticas que regulan el uso de estos recursos. Al ingresar a la Red, el usuario asume toda responsabilidad legal que surja de una violación a estas políticas.

6. Definiciones

- **Grupo de Tecnología de la Información (TI) –** Oficina encargada del manejo y administración de la infraestructura de telecomunicaciones y equipos tecnológicos administrativos del IDCBIS.
- **Redes de Telecomunicaciones –** Conjunto de todas las infraestructuras tecnológicas que provean comunicaciones de voz, de datos, conectividad a Internet, acceso y control de sistemas centralizados de datos, sistemas de correo electrónico, aplicaciones de red, pagina Web pública, y todos los archivos e información obtenida, accedida o archivada en los sistemas antes mencionados.
- **Computadoras / Computadoras Portátiles –** Todo equipo de computación utilizado por el personal del instituto en la realización de sus labores que permita el acceso a las Redes de Telecomunicaciones, las aplicaciones instaladas en ese equipo, y la información contenida, accedida u obtenida en dicho equipo.
- **Usuarios –** Todo personal administrativo, personal académico y personal externo que esté autorizado a acceder las Redes de Telecomunicaciones.
- **IDCBIS / Instituto –** Se refiere a todos los recintos y facilidades del Instituto Distrital de Ciencia Biotecnología e Innovación en Salud.
- **Confidencialidad –**los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
- **Integridad –** El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
- **Disponibilidad –** Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.
- **Propietario de Activos de Información –** en el contexto de la norma NTC 27001, un propietario de activos de información es cualquier persona o entidad a la cual se le asigna la responsabilidad formal de custodiar y asegurar un activo de información o un conjunto de ellos.
- **Activo de información –** recurso de información que tiene valor para la entidad.
- **Activos de software - e**lementos de software de gran valor para la Entidad, como las herramientas ofimáticas, sistemas manejadores de bases de datos, aplicaciones de software específico, software del sistema y herramientas de desarrollo.

7. Marco Legal

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2

8. Clasificación y control de activos

8.1. Activos de información

Cada área del instituto, debe elaborar y mantener un inventario de los activos de información (ver su definición en definiciones) que poseen (procesada y producida). Las características del inventario, donde se incorpore la clasificación, valoración, ubicación y acceso de la información, las especifica el grupo de TI, correspondiendo igualmente brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

8.1.1. Políticas de seguridad de activos de información.

Protección y respaldo de la información

- Los niveles de protección y clasificación establecidos para la información de la institución deberán ser mantenidos en todo momento. (Acceso, toma de respaldo, backup, transporte, recuperación, otros). Por lo tanto, se deben mantener los controles y medidas establecidas para esto.

- Los usuarios respaldarán y protegerán, con medidas que eviten accesos de personas no autorizadas, aquellos activos digitales de información que estén almacenados en elementos de TI de uso personal, que les hayan sido asignados (CD, USB, Disco externo etc.).

- Se deberán preservar los lineamientos de acuerdo a la sensibilidad y nivel de clasificación de seguridad. Las copias de seguridad o backup de la información que no se encuentren respaldado en el esquema de backup será asumido por el usuario, quien es el único responsable.

- Los usuarios son responsables de aplicar los controles para la protección de la información según su nivel de clasificación. Así mismo deberán alertar al grupo TI cuando un activo digital de información requiera medidas especiales de protección.

8.2. Activos de Software

8.2.1. Políticas de seguridad de activos de software

- Los medios, documentos o licencias de software deben están custodiados por un referente y almacenados en un lugar seguro donde no se tenga acceso por personal externo al grupo de TI.
- La gestión y/o administración de las licencias de software deben ser de responsabilidad del grupo de TI.
- Se debe contar con un directorio (DML - Biblioteca Definitiva de Medios) para almacenar los medios magnéticos para la instalación de software licenciado por él IDCBIS.

9. Seguridad ligada al personal

9.1. Acuerdos de confidencialidad

Todos los funcionarios del instituto y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la Institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos del IDCBIS a personas o entidades externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

9.2. Derechos y obligaciones de los funcionarios

- El propósito principal, de los datos, recursos y servicios informáticos, es el de contribuir al cumplimiento de objetivos del IDCBIS, por ello, todas las personas (funcionarios y contratistas), que los utilicen deben estar de acuerdo y compartir este propósito. En efecto, se espera y así se exige, que, quien los utilice, actúe acorde con este propósito y lo haga con suma responsabilidad, incluyendo el cuidado físico de los mismos. Los Usuarios asumen la responsabilidad de conocer, entender y seguir los procedimientos administrativos, establecidos cumpliendo con las directrices administrativas trazadas para tal fin.
- Sin perjuicio de las normas Constitucionales, legales y reglamentarias que regulan la materia, cada Usuario asume individual y solidariamente, toda responsabilidad derivada de los daños y perjuicios que el mal uso de las TIC y de la información puedan hacer.
- Cada Gestor o líder de área es el responsable de solicitar y cancelar ante el grupo de TI los recursos de hardware, software o servicios que requiera el funcionario o contratista a su cargo mediante el sistema de mesa de ayuda:

  Computador, impresora, cuenta de red, correo electrónico, claves, sistemas de información, Group directory "X:", acceso a carpetas (privada o públicas de cada dependencia).
- Es responsabilidad del Gestor o líder inmediato de un Usuario, solicitar formalmente al grupo de TI, los

perfiles de usuario con sus privilegios, de acuerdo con el tipo de información que requiera operar y a su vez la cancelación cuando ya no los estime convenientes o necesarios

- Es responsabilidad del grupo de Innovación y Desarrollo solicitar la cancelación de las cuentas de red, correo electrónico y demás permisos que tenga un usuario a su cargo en el momento de su terminación de contrato o retiro, de no hacerlo, el Gestor o líder inmediato, lo podrá solicitar.
- Es obligación del Gestor o líder inmediato, informar previamente a los usuarios sobre la información que está clasificada como confidencial y qué medidas de seguridad se deben tener para el manejo y disposición de datos e información.
- Para todo funcionario, no está permitido compartir claves de usuarios o de aplicativos. El nombre de usuario y la clave de acceso asignados a un funcionario, son personales e intransferibles. La autorización de acceso a los recursos es exclusiva al usuario al que le fue asignada y no es transferible ni heredable a otros usuarios o dispositivos.
- Ningún funcionario podrá hacer utilización de cualquier recurso informático de la Red del IDCBIS, con propósitos comerciales en beneficio del Usuario y/o de terceros.
- Para todo funcionario, no está permitido la utilización de cualquier recurso informático de la Red de una manera que viole cualquier norma Nacional o Internacional.
- Ningún funcionario está autorizado a realizar instalaciones de hardware y/o software sin la autorización del grupo de TI.
- No se autoriza a ningún funcionario permitir a personal externo acceder a recursos informáticos con su usuario y clave personal.

9.3. Carpetas compartidas en la red de datos y/o en aplicativos.

- Es responsabilidad del Gestor o líder del área funcional dar la autorización de asignación de permisos a los contratistas, sobre los recursos TI de su dependencia y estos son los responsables por las acciones y los accesos sobre la información que se presenten en el desarrollo de las funciones realizadas, en las carpetas compartidas en la red o en aplicativos.
- El grupo TI implementa, en los casos aprobados, la configuración de acceso a las carpetas compartidas en la red y en aplicativos, previo requerimiento formal de la misma a través de la herramienta Mesa de ayuda dispuesta para tal fin.
- Es responsabilidad de cada dependencia mantener depurada la información almacenada en las carpetas compartidas en la red o en aplicativos para la optimización del uso de los recursos de almacenamiento.
- La entidad cuenta con carpetas compartidas en la red denominadas carpetas compartidas, la cual hace parte del esquema de backup, es decir la información es respaldada a través de copias de seguridad a excepción

de carpetas públicas, esta última no tiene respaldo.

10. Seguridad física y del entorno

10.1. Seguridad de áreas

10.1.1. Controles físicos de entrada.

- Cualquier persona "interna o externa", que ingresa a la entidad con equipos de cómputo portátiles o de escritorio, debe realizar el respectivo registro de los equipos en los puestos de vigilancia de las instalaciones. Los vigilantes revisarán los bolsos, maletines, paquetes extraídos por colaboradores y visitantes, de las instalaciones del IDCBIS.
- Todos los colaboradores deben ingresar a las instalaciones del IDCBIS validando su ingreso con el carnet asignado para tal fin. Los visitantes serán registrados en el sistema correspondiente, con su número de identificación, hora de ingreso y dependencia hacia la cual se dirigen.

10.1.2. Seguridad centro de cómputo.

- Actualmente el IDCBIS no cuenta con centro de cómputo dado su actual eco dependencia con la Secretaria de Salud, mediante el actual contrato de comodato.

10.1.3. Seguridad centros de cableado.

- A los centros de cableado solo podrá ingresar el personal de TI autorizado para dicho fin y mediante previa solicitud de apertura al personal de TI de la Secretaria de Salud.
- El ingreso de personal externo (proveedores, consultores, directivos etc.), debe realizarse con el acompañamiento de una de las personas autorizadas.

10.1.4. Seguridad áreas de procesamiento de información.

- Las áreas en las cuales se procesa información sensible de gestión del instituto, se protegerán con controles físicos de acceso adicionales, con el fin de evitar el acceso, modificación o sustracción de los datos procesados, sea por personal interno o externo del instituto.

11. Gestión de comunicaciones y operaciones

11.1. Gestión de la seguridad en red.

- Todos los requerimientos sobre compra, arriendo, préstamo, donación etc. de cualquier tipo de equipo o elemento tecnológico, deberá canalizarse en forma oportuna a través del grupo de TI, quien revisará su pertinencia, conveniencia, compatibilidad, disponibilidad de recursos y procederá a conceptuar y/o a la provisión correspondiente.
- No se permite realizar conexiones no autorizadas a la red, tanto alámbrica como inalámbrica.
- No está permitido que un funcionario del IDCBIS, prive o intente privar a otros usuarios de la utilización y/o acceso a recursos informáticos de la Red que estén autorizados.

- No se permite a ningún funcionario penetrar o intentar penetrar sin autorización, la seguridad de cualquier comunicación de la red.
- Cualquier trabajo de adición de puntos de red en el cableado estructurado del IDCBIS, deberá tener el apoyo técnico y acompañamiento del grupo de TI, con el fin de garantizar el cumplimiento del estándar establecido e implementado por la entidad, en donde se especifican las condiciones y características del cableado a instalar.

11.2. Gestión de la seguridad en el manejo del correo electrónico.

- Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de correo electrónico del instituto.
- La cuenta de correo electrónico es personal e intransferible. El usuario se compromete a hacer un uso diligente de la cuenta y a mantener su contraseña en secreto. Así mismo, el usuario se compromete a notificar al grupo de TI de manera inmediata la pérdida de su contraseña o acceso no autorizado por parte de terceros a su cuenta.
- Es necesario que la primera vez que el usuario reciba su cuenta de correo cambie su clave. Además, por motivos de seguridad, se recomienda cambiar la clave, como mínimo, cada tres meses.
- El correo electrónico es una herramienta para el intercambio de información entre personas, no es una herramienta de difusión masiva e indiscriminada de información.
- los colaboradores del instituto deben evitar abrir los archivos adjuntos en mensajes de remitentes desconocidos o sospechosos.
- La falta de uso de la cuenta de correo supone su desactivación. Se considera falta de uso no haber accedido a ella durante más de 3 meses. Una cuenta desactivada deberá activarse para volver a estar operativa. Mientras la cuenta permanezca desactivada no podrá recibir ningún mensaje.
- Es responsabilidad de cada usuario tener copias de respaldo (Backups) de los mensajes de sus carpetas de correo y de su agenda de direcciones electrónicas, de ser necesario. Estos datos, para efectos legales, se consideran en tránsito y temporales, por tal razón no se respaldan por parte del grupo de TI.
- Para asegurar el buen funcionamiento del servicio y un uso eficiente de los recursos del sistema de correo, el usuario se compromete a:
    - Leer periódicamente su correo.
    - No utilizar las cuentas de otros usuarios.
    - Usar un lenguaje apropiado en sus mensajes.
    - Ceñirse a las normas y conductas de cortesía de uso de correo electrónico.
    - No mandar ni contestar cadenas de correo o cualquier otro esquema de "pirámide" de

mensajes.

- Informar al administrador del Servicio de Correo Electrónico sobre aquellos casos de abuso de correo que detecte para evitar que vuelvan a suceder al mismo o a otros usuarios.

- No está permitido:
  - Usar la cuenta para fines comerciales o particulares.
  - Transmitir virus, programas de uso mal intencionado o introducir software malicioso en la red o en los servidores (virus, worms, ráfagas de correo electrónico no solicitado, etc).
  - Leer correo ajeno, generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.
  - Enviar mensajes con direcciones no asignadas por los responsables de nuestra institución y en general es ilegal manipular las cabeceras de correo electrónico saliente.
  - Violar los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual.
  - Usar el sistema con el fin de realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil o maliciosa.
  - Enviar mensajes de correo no solicitados, incluyendo junk mail (material publicitario enviado por correo) o cualquier otro tipo de anuncio comercial (email spam, mensajes electrónicos masivos, no solicitados y no autorizados en el correo electrónico).
  - Enviar mensajes de correo masivo, no relacionados con las actividades de la Secretaría, a un gran número de grupos de noticias (newsgroup, spam, mensajes electrónicos masivos, no solicitados y no autorizados en grupos de noticias).
  - Si, en el ejercicio de sus funciones, el personal del grupo de TI detecta cualquier anomalía que muestre indicios de usos ilícitos, lo pondrá en conocimiento de la autoridad competente del IDCBIS y, si procede, de la autoridad judicial.
  - Enviar archivos adjuntos de gran tamaño, que puedan congestionar la red. Los usuarios podrán hacer uso de recursos compartidos destinados para intercambiar información laboral importante.
  - Incluir en la firma del correo electrónico dibujos, banners, animaciones o frases que no pertenezcan al formato estándar establecido de firma del correo institucional.

12. Control de acceso a los sistemas de información

12.1. Requisitos para el control de acceso.

- Todos los usuarios que acceden a recursos de TI de la red interna del IDCBIS, requieren de una única e intransferible identidad, normalmente un nombre de usuario para una única persona, y un nombre de

máquina para un PC. Esta identidad se usa para representar un usuario o dispositivo en el ambiente informático de la red. El grupo de TI proporcionará este identificador como parte del proceso de autorización. Todas las acciones realizadas bajo los auspicios de un identificador de usuario y sus consecuencias legales son responsabilidad del usuario titular del identificador.

12.2. Gestión de acceso de usuarios

- El grupo de TI debe garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los servicios de red y a los sistemas de información.
- La asignación de cuenta de usuario se realizara mediante la solicitud de creación de cuenta ante la mesa de ayuda de la secretaria de salud de acuerdo al actual contrato de comodato por parte del grupo de TI del IDCBIS, posterior el grupo de TI asignara los identificadores de acceso al usuario final.
- En la activación de usuarios de correos electrónicos, se crearán identificadores de usuario utilizando el estándar de la letra inicial del nombre seguida del primer apellido, en caso de que el usuario ya exista se tomara la primera letra del segundo nombre o en su defecto el número 1.
- El encargado de TI no cambiará ninguna clave de acceso, si no es por solicitud expresa del respectivo usuario.
- Cada usuario generará sus propias claves de acceso, cada cierto período de tiempo en la medida que las posibilidades técnicas que así lo permitan. Las conformará mediante el empleo de letras mayúsculas, minúsculas y números. El período lo establecerá el grupo de TI, dependiendo de la sensibilidad de la información.
- El usuario no debe dejar las claves de acceso escritas en medios o lugares donde puedan ser obtenidas por terceros (Ej.: monitor, carpetas, escritorio).
- Cuando el usuario olvide u extravié su clave de acceso, deberá acudir al grupo de TI e identificarse como propietario de la cuenta para que se le proporcione una nueva, o la utilización de cualquier otro medio de verificación que el Grupo de TI defina para la restauración de contraseñas.
- Es responsabilidad del director, gestor o líder inmediato, informar la des-habilitación de la cuenta de usuario por motivo de la no permanencia del funcionario en la entidad o por no necesitar dichos recursos.
- Los usuarios deberán aplicar medidas preventivas cuando se ausentan de las labores, antes de retirarse del lugar de trabajo donde se ubique el equipo de cómputo, el usuario deberá tomar las siguientes precauciones mínimas:
    - Concluir las sesiones activas de cualquier sistema informático al finalizar las tareas;
    - Proteger el equipo contra usos no autorizados mediante un mecanismo de bloqueo de seguridad autorizado por la Institución;
    - Cerrar la conexión con los servidores.

- El grupo de TI debe aplicar el control de deshabilitar la cuenta de usuario de los sistemas de información por inactividad mayor a treinta (30) días calendario.

12.3. Responsabilidad de los usuarios.

- No está permitido a terceros, el ingreso a los recursos tecnológicos del IDCBIS sin autorización previa del gestor o líder inmediato o el supervisor del contrato.

- Está prohibido el almacenamiento, la transmisión, transferencia y, difusión de datos de carácter personal en los equipos del IDCBIS.

12.4. Control de acceso a la red.

- El mal uso de la identidad de un usuario o un dispositivo constituye falsificación o falsedad. Sin perjuicio de las acciones legales, toda acción que involucre acceso desautorizado, impropio o el mal uso de recursos informáticos de la red interna del IDCBIS, está sujeta a sanciones disciplinarias o legales pertinentes.

12.5. Control de accesos al sistema operativo.

- No se permite alterar la configuración del software de los equipos, Sistema Operativo, Motores de Base de Datos, Herramientas de Desarrollo, Utilitarios del Sistema, Software de Comunicaciones de un PC o de la Red, sin previa autorización del grupo de TI.
- En las estaciones de usuario final se tendrán como estándar un usuario genérico con perfil de administrador local, no se podrán adicionar y/o configurar usuarios con privilegios de administración local. Ante una solicitud de adicionar a la maquina un usuario de la red con privilegios de administración local, esta solicitud deberá ser enviada previamente por el jefe inmediato y escalada al grupo de TI, quien evaluará y analizará si el usuario, dentro de las actividades propias de sus funciones, requiere este perfil o nivel de permisos.

- La activación y desactivación de usuarios de sistemas operativos estará a cargo del personal técnico del grupo de TI.

- Siempre que los sistemas operativos utilizados lo permitan, deberá controlarse el número de intentos de ingreso fallidos. Luego de 8 intentos, deberá bloquearse la cuenta del usuario y no permitir su ingreso al sistema. Solo el administrador de TI podría desbloquearla antes por solicitud del usuario involucrado mediante la mesa de ayuda.

- En el caso que el sistema operativo lo permita, se deberán implementar las bitácoras de seguimiento a los accesos, donde se registren los ingresos al sistema y los intentos fallidos.

12.6. Control de acceso a aplicaciones e información.

- A todo colaborador y proveedor de servicios del IDCBIS, no está permitido el uso no autorizado de cuentas de red y de computadores u otras formas de acceso a los recursos informáticos.
- Los dispositivos y sistemas conectados a la Red deben, en todo momento, estar por completo de conformidad con las licencias de software adquiridas y disponibles en el IDCBIS.
- Es responsabilidad de los gestores o líderes de área la definición y ejecución de procedimientos que contemplen la segregación de funciones necesaria para garantizar un acceso y gestión segura de la información confidencial, reduciendo los riesgos de errores, fraudes, uso o sustracción no autorizada de datos.

12.7. Control de acceso a computación móvil (Wireless).

- La red inalámbrica del IDCBIS usara el estándar 802.11a/b/g/ac. Por lo tanto, las tarjetas de red inalámbrica deben poseer la certificación Wi-Fi™ de este estándar.
- La institución definirá redes inalámbricas, con propósito específicos:
    - Privada, Corresponde a usuarios internos “funcionarios” que se conectarán a la red autenticándose ante el dominio de la entidad, aplicándole así todas las políticas y directivas institucionales definidas en el Directorio Activo,
    - Invitados, corresponde a usuarios externos que no se autenticarán ante el controlador de la red inalámbrica, no tendrán acceso a la red interna, solo tendrán salida a internet y la navegación será controlada por las políticas de la entidad.
- Los equipos externos, “entiéndase por cualquier equipo de cómputo portátil que ingresa al IDCBIS por parte de proveedores, visitantes o equipos personales de funcionarios y/o contratistas, que no son de propiedad de la entidad y no están como equipos miembros del dominio”, no podrán ser conectados a ninguno de los puertos de la red LAN de la entidad y cualquier intención de conexión será tomado como un intento de acceso no autorizado. Estos equipos solo se podrán conectarse inalámbricamente a la de invitados, que será designada para prestar el servicio de navegación hacia internet sin tener acceso a la red interna.
- No está permitida la instalación de dispositivos inalámbricos que brinden acceso inalámbrico a la red sin la debida autorización del grupo de TI.
- El IDCBIS no controla ni es responsable del contenido y veracidad de la información que se transporta en la red interna, en consecuencia, los usuarios son responsables por la utilización el servicio de manera apropiada.
- Los usuarios de la red interna, son responsables de la seguridad de la información en las transacciones que envíen por la Red Inalámbrica. Por tanto, se recomienda que utilicen aplicaciones seguras (secure shell,

https, etc.).

- En conocimiento que las redes inalámbricas son fundamentalmente inseguras, en virtud de que el envío de la información se realiza por un medio compartido, por consiguiente, recomienda abstenerse de realizar transacciones bancarias o similares, ya que no es posible por dicho medio garantizar la seguridad de las transmisiones.
- Todo funcionario y/o usuario debe abstenerse de publicar o pasar a terceros no autorizados por el IDCBIS, las claves e información de acceso a la red o de obtenerlas o decodificarlas en caso de que no se les proporcione directamente por la entidad.
- No está permitido el uso de la red interna, con fines de lucro o propósitos comerciales que no estén directamente relacionados con asuntos que la propia entidad autorice, difunda y solicite.
- No se permite descargar servicios de difusión o broadcast, tales como audio y video.
- No está permitido usar programas "peer to peer" (P2P) o alguna otra tecnología que permita el intercambio de archivos en volumen.
- No está permitido extender el servicio de acceso a la red interna a más equipos por medio de conexiones a la red inalámbrica no autorizadas para éste fin (ej: por medio de NAT, túneles, conexión compartida a internet, etc.) y/o extender el alcance de la red por medio de cualquier dispositivo físico o lógico (tales como antenas o repetidores) más allá de la superficie o límite físico de la entidad.
- No se autoriza obtener acceso a cualquier recurso computacional, sistema o sitio de telecomunicaciones a los que no le está permitido acceder.
- No se permite realizar actividades de rastreo, ataques de negación de servicio, difusión de virus, spyware o programas considerados dañinos o inapropiados o cualquier otra actividad informática ilícita.
- El grupo de TI se reserva el derecho de controlar o negar el acceso al servicio de la red interna a aquellas personas que no cumplan con los requisitos de uso establecidos en esta política.

13. Desarrollo y mantenimiento de sistemas.

13.1. Especificaciones y requisitos para la adquisición desarrollo y mantenimiento de sistemas de información.

- Todo desarrollo, cambio, actualización, compra, mejora o implantación de Software deberá solicitarse oportunamente a través del grupo de TI.
- No está permitida la creación de archivos de copias de seguridad en los servidores que son accesibles desde redes externas.
- Para la publicación de páginas web de la entidad, se debe restringir o eliminar el acceso a directorios sensibles que contengan información como bases de datos o páginas de administración.

- Para la publicación de páginas web de la entidad, se debe implementar certificados de cifrados de seguridad SSL de encriptación robusta.

13.2. Seguridad sistemas de información y de datos de los mismos.

- Los sistemas de información del IDCBIS deben tener ambientes separados de desarrollo, pruebas y operación, con el fin de garantizar su integridad y correcto funcionamiento.
- El referente del ambiente de producción de un sistema de información, es el jefe de grupo o de dependencia, y por ningún motivo, funcionarios diferentes a los asignados por él, tendrán acceso a la información y/o aplicativos que reposen en este ambiente. Así mismo, será el encargado de aprobar formalmente los cambios o nuevas implantaciones, módulos o nuevos procedimientos. Se deben implementar los controles necesarios para garantizar que solamente los colaboradores autorizados tengan acceso a los códigos fuente.
- Ante la eventual celebración de un contrato con una persona natural o jurídica que con ocasión al desarrollo de su objeto contractual requiera acceso a información del IDBIS y que esté almacenada en bases de datos; para el efecto solo se suministrará una muestra, protegiendo los datos de los usuarios o evento, evitando su identificación. Cuando se trate de información con la cual el contratista requiere datos de usuario o evento se aplicarán cláusulas de confidencialidad, para evitar que se realice un uso indebido de la información; lo que incluye que la información o bases de datos suministradas no pueden ser retiradas de la institución o reproducirse en servidores que no pertenezcan a la entidad o en PC internos o externos. Así mismo se debe advertir que no se pueden sustraer copias totales o parciales de los datos en otros formatos, como archivos planos. No obstante, ante el evento de ser necesaria una copia, ésta se debe requerir a través del supervisor del contrato o del jefe inmediato.
- Una vez que un contratista o funcionario termine su vínculo contractual o laboral y/o suspenda la ejecución de su contrato o funciones y que, con ocasión a las actividades, accedió mediante usuario a las bases de datos mencionadas en el numeral anterior, el supervisor o jefe inmediato deberá solicitar el retiro de los permisos o accesos autorizados.

  Nota: Para retirar los permisos o accesos autorizados se ha de tener en cuenta que también se debe inhabilitar a nivel de base de datos. Cuando se trate de una cuenta asignada a un sistema gestor de bases de datos, se debe solicitar al usuario la información de las cuentas a su cargo, ya sea para inactivarlas o proceder al proceso de cambios de clave.

- Los usuarios a quienes se les ha asignado permisos de acceso a los sistemas de información; son

responsables de la modificación, actualización, copia, lectura de los datos contenidos en las bases de datos.

- Cada referente de un sistema de información, es responsable de la asignación de permisos que se conceden a los usuarios y funcionarios, por lo que se debe otorgar el mínimo de privilegios (permisos de acceso), teniendo como base el análisis previo a las necesidades y actividades a realizar.
- Ante la necesidad de divulgar o publicar de manera parcial o total datos o información del IDCBIS, es necesaria la autorización previa del jefe inmediato responsable del sistema de información, lo anterior de conformidad con lo dispuesto en la Ley 1266 de 2008 o Ley de Habeas Data.
- El administrador de las bases de datos, no puede suministrar información de las bases de datos que administra, sin previa autorización del supervisor o jefe inmediato.

14. Gestión de incidentes

Se consideran incidentes de seguridad de la información las siguientes conductas, prohibidas para cualquier colaborador o tercero que haga parte en procesos para y/o del IDCBIS:

- La utilización de técnicas y/o herramientas de “Hacking”.
- La ingeniería inversa, cracking o descriptación de contraseñas.
- El escaneo de puertos de TCP/IP.
- La sustitución de usuarios o Hacking.
- La sustitución de paquetes IP, también conocida como IP spoofing
- La utilización de analizadores de protocolos o scanners de tráfico de red.
- Grabadoras de teclas o Key Loggers
- Hardware para ataques de Tempesting.
- Herramientas de denegación de servicio.
- Utilización de identificadores de usuarios ajenos al IDCBIS,
- Hacer ingeniería social.
- El uso de computadoras como gateways o routers a otra red o como servidor de acceso remoto, se requiere en todo caso autorización previa y expresa del grupo de TI.
- Crear, utilizar o distribuir programas como virus, troyanos, key loggers etc., que puedan causar daño a datos, archivos, aplicaciones, funcionamientos de los sistemas o alteren el funcionamiento de la red.
- Capturar, desencriptar, difundir contraseñas y/o protocolos de comunicaciones.
- Inspeccionar, modificar o copiar programas o datos sin la autorización del jefe inmediato o que atenten contra las

normas legales y reglamentarias vigentes sobre

- utilización de software y/o propiedad intelectual.
- Utilizar cualquier correo electrónico o sistema de mensajería, para enviar contenido abusivo, ofensivo, obsceno, subversivo o saturar los canales de comunicaciones, o el envío “cadenas de cartas”, y otros esquemas que pueden causar tráfico excesivo en la red o cargar los sistemas informáticos.
- Utilización de cualquier recurso informático de la red para generar, guardar o transportar material ilegal, pornográfico, que haga apología del crimen o violencia, ofensivo, lesivo al buen nombre y honor del instituto, o cualquiera persona, propagandas comerciales, cadenas, difusión de actividades lucrativas en general, ni para actividad no administrativa o de servicio, proselitismo político.
- Alterar el software o la configuración del hardware de cualquier equipo o computador o agregar cualquier dispositivo o sistema a la red sin el permiso correspondiente.
- Utilización de software comercial que no esté licenciado, ya sea texto, imágenes gráficas, o grabaciones de audio o video.
- Utilización de la Red para ganar o intentar ganar el acceso desautorizado a los recursos de información locales o remotos.
- Posesión o utilización de cualquier software o hardware que pueda comprometer la seguridad de la red y/o de cualquier recurso informático de la Red.

15. Gestión de los incidentes:

- Es responsabilidad de los colaboradores del IDCBIS reportar las situaciones consideradas como incidentes de seguridad, anteriormente descritas, de las cuales tengan conocimiento, al grupo de TI.
- El grupo de TI tomará las medidas apropiadas para mitigar los riesgos generados por el incidente presentado.
- Los usuarios en cuyos dispositivos de almacenamiento, discos, group directory (X:), carpetas públicas o privadas de las dependencias, se encuentre software no autorizado, archivos de música, videos, fotografías no institucionales, se les procederá a borrar dichos archivos sin previo aviso, y el grupo de TI podrá dirigir estos hallazgos a la dependencia competente para que se proceda a dar curso a las investigaciones a que dieran lugar.

16. Políticas de seguridad para el manejo de computadores con información confidencial.

- No está permitido en los computadores utilizados para el manejo de información confidencial tener habilitados puertos USB, unidades de CD o DVD o cualquier otro puerto que permita la grabación de información. Tampoco pueden tener la opción de impresión de documentos.

- No está permitido en los computadores utilizados para el manejo de información confidencial tener acceso a Internet.
- Los computadores utilizados para el manejo de información confidencial no pueden ser reubicados sin permiso del gestor o líder inmediato.
- La pérdida o robo de cualquier componente de hardware o programa de software en computadores utilizados para el manejo de información confidencial debe ser reportada inmediatamente al grupo de TI.
- Para prevenir el acceso no autorizado, se usará un sistema de contraseñas robusto y se debe configurar el protector de pantalla para que se active al cabo de 3 minutos de inactividad y que requiera una contraseña al retomar la actividad. Además, el usuario debe activar el protector de pantalla, bloqueando su sesión manualmente, cada vez que se ausente de su lugar de trabajo u oficina.
- Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas, mediante disposición apropiada del mobiliario de la oficina y protector de pantalla.
- Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.
- Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems o dispositivos de comunicación inalámbrica en PC que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Entidad.
- Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al grupo de TI y poner el computador en cuarentena, hasta que el problema sea resuelto.
- Siempre que sea posible, debe eliminarse información confidencial de los computadores y unidades de disco duro antes de realizar operaciones de mantenimiento correctivo y/o preventivo. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de un representante del grupo de TI.
- Los equipos de cómputo que sean reasignados o dados de baja serán revisados y formateados por parte del grupo de TI para eliminar todo rastro de información confidencial que pueda ser accedida por personal no autorizado o externos al IDBIS, para ello, el jefe del área que requiera la novedad, debe realizar el requerimiento a la Mesa de Servicios.

17. Políticas de uso de los dispositivos móviles.

- El aseguramiento de la administración de los recursos de dispositivos móviles como teléfonos, tablets etc., pertenecientes al IDBIS será administrado por el personal especializado, designado por el grupo TI.
- La Dirección de TI establecerá y aplicará un procedimiento de instalación y configuración de las aplicaciones móviles, a través de la herramienta de gestión designada para ello.
- Toda solicitud de servicio, Incidente, cambio y/o problema, realizado sobre el servicio, debe ser atendido por medio de un caso reportado el sistema de mesa de ayuda.

17.1. Controles Físicos

- El personal protegerá sus equipos móviles, haciendo uso personal e intransferible de ellos, en particular en aquellos dispositivos inteligentes que almacenan información sensible de la Entidad. En estos casos, incluso los mensajes recibidos de números o remitentes desconocidos deber ser ignorados y borrados sin ser abiertos.

17.2. Autenticación y Acceso

- Se protegerá el acceso a los dispositivos móviles según los privilegios de cada perfil de usuario (Password, tokens, huella digital, etc.). Las capacidades del equipo respecto del control de acceso serán definidas en función de la importancia de la información que se almacena o se protege en cada equipo.

17.3. Parches y Actualización

- Todos los usuarios de dispositivos móviles que contenga información altamente confidencial o crítica de la entidad, utilizarán la última o la más segura versión de las aplicaciones.

18. Historial de Revisión de Actualización

Historial de Revisión de Actualización		
Versión	Descripción de la Actualización	Fecha
1.0	Política Nueva	01/09/2018

19. Aprobaciones

Redactado Por:	**Ing. Lupoani Sánchez Méndez Gestor de Tecnologías de la Información**	**01/09/2018** **Fecha**
Revisado Por:		**Fecha**
Revisado Por:	**Dr. Bernardo Camacho, Director Ejecutivo Instituto Distrital de Ciencia Biotecnología e Innovación en Salud (IDCBIS)**	**Fecha**
Aprobado Por:		**Fecha**