# MANUAL DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO DE DESARROLLO DE ARAUCA – IDEAR

## Contenido

## TITULO I
## GENERALIDADES

**Artículo 1. Objeto Social.** El Instituto de Desarrollo de Arauca, IDEAR, tendrá por objeto principal el fomento del desarrollo económico y social en el ámbito local, municipal, departamental y regional mediante la prestación de servicios relacionados con la ejecución de actividades financieras y las conexas para ejecutar estas, dirigidas a la obtención, administración y colocación de recursos que se utilicen para gestión y ejecución de programas y proyectos de inversión en los sectores económicos y sociales destinatarios, constitucional y legalmente de la inversión Estatal; todo lo anterior en el marco legal que como establecimiento público del orden territorial le corresponde y puede desplegar al pertenecer a la categoría de instituto para el financiamiento y desarrollo territorial.

**Artículo 2. Misión**. La Misión del Instituto de Desarrollo de Arauca, IDEAR, consiste en contribuir con el fomento del desarrollo económico y bienestar social del Departamento de Arauca, a través de la ejecución de las actividades financieras y gestión de programas y proyectos de inversión que, en el marco legal vigente, puede desplegar como establecimiento público del orden territorial y su categoría de Instituto para el Financiamiento y Desarrollo Territorial, INFIS.

**Artículo 3. Visión**. El Instituto de Desarrollo de Arauca, IDEAR, se consolidará como una entidad líder del nivel descentralizado departamental, consecuencia de la implementación de su modelo de gestión y financiamiento de proyectos socioeconómicos, que promuevan el bienestar de la región y garanticen su sostenimiento con rentabilidad en el contexto social e institucional.

**Artículo 4. Naturaleza Jurídica**. El Instituto de Desarrollo de Arauca, IDEAR, es un establecimiento público de carácter departamental, descentralizado, así como de fomento, promoción y desarrollo social, regulado por los artículos 70 a 81 de la Ley 489 de 1998 y el Decreto Nro. 1221 de 1986, dotado con personería jurídica, autonomía administrativa y patrimonio propio. Además, hace parte de las instituciones denominadas en el Estado Colombiano como Institutos de Fomento y Desarrollo Territorial, INFIS.

**Artículo 5. Funciones**. En desarrollo de sus objetivos el Instituto ejercerá las siguientes funciones.

1. Conceder créditos a entidades públicas y a particulares que presten servicios públicos, dirigidos a proveer recursos para impulsar programas de desarrollo, así como proyectos de inversión en los sectores económicos y sociales destinatarios, constitucional y legalmente de la inversión Estatal; de igual manera ejecutar en calidad de entidad proveedora de recursos o entidad prestataria, operaciones de crédito público, las operaciones asimiladas a éstas y las operaciones propias del manejo de la deuda pública y las conexas.

2. Realizar operaciones de redescuento y sus operaciones conexas ante los organismos de carácter público o mixto, nacionales o internacionales, actuando como intermediario de captación de esos recursos en favor de promover la ejecución de programas de desarrollo y proyectos de inversión en los sectores tanto económicos como sociales destinatarios constitucional y legalmente de la inversión Estatal.

3. Obtener y administrar los recursos que se refieran a excedentes de liquidez de las entidades territoriales de la jurisdicción departamental, siempre y cuando se cumplan con las condiciones administrativas y financieras que establecen las disposiciones legales vigentes.

4. Actuar como entidad operadora de libranza o descuento directo, señalado en la Ley 1527 de 2012 o las disposiciones que la modifiquen o sustituyan.

5. Realizar operaciones financieras de descuentos de sus acreencias y tramitar redescuento de las mismas.

6. Servir de garante de las obligaciones crediticias asumidas por entidades de derecho público del territorio departamental, cuando estas realicen la obtención de esos recursos para la ejecución de proyectos de inversión de obras públicas, condicionando aquel servicio a la constitución a su favor de la garantía idónea y suficiente que sea factible para la respectiva entidad pública.

7. Prestar servicios de asesoría, así como de cooperación técnica y financiera, a las entidades territoriales del departamento y sus entes descentralizados, en los proyectos de inversión financiados con recursos del Instituto o cuando se trate de otras fuentes de financiación.

8. Prestar a las entidades territoriales del departamento y sus entes descentralizados los servicios técnicos de capacitación, asesoría y apoyo, bien sea directamente o mediante los sistemas y mecanismos que se determinen en los manuales de crédito, para el ejercicio de la supervisión y seguimiento de los proyectos o programas financiados con recursos del Instituto, o cuando se trate de otras fuentes de financiación.

9. Aunar esfuerzos económicos y administrativos para la ejecución de programas y proyectos de inversión, que interesen al Departamento y sus municipios a través de la ejecución permanente de gestión e interacción con las entidades que en el ámbito nacional, regional, departamental y municipal propicien en forma directa el desarrollo de la región.

10. Proponer a las administraciones municipales, a la departamental y la nacional, al igual que a las instancias institucionales conformadas por estas, la aplicación de herramientas de capacitación, investigación, alianzas institucionales, entre otras, que estén dirigidas a identificar las necesidades técnicas, financieras y de inversión que conlleven al desarrollo de la productividad de los sectores económicos con presencia e importancia en la región.

11. Coadyuvar al Gobierno Departamental en la ejecución de los planes, políticas y programas de desarrollo integral, mediante la prestación de los servicios que constituyen su objeto.

12. Recibir y mantener los recursos destinados por la Nación, el Departamento y los Municipios al funcionamiento y ejecución de obras, planes, proyectos y programas hasta tanto se requieran para efectuar su inversión por la entidad destinataria de los mismos, de acuerdo con los parámetros legales.

13. Realizar la formulación, administración y ejecución de los proyectos de Asociaciones Público-Privadas (APP) que realicen los usuarios que conforman su población objetivo, de acuerdo con lo establecido en el Artículo 37 de la Ley 1508 de 2012.

14. Asesorar técnicamente la estructuración, formulación, viabilidad y ejecución de proyectos factibles de financiar con recursos del Sistema General de Regalías, en los términos señalados en los artículos 25 y 28 de la Ley 1530 de 2011 y otras fuentes de financiación.

15. Ejecución de las estrategias señaladas a cargo de las entidades territoriales en las leyes que adopten los planes nacionales de desarrollo, y que se relacionen con la gestión, el mejoramiento de competitividad e infraestructura regional, la tecnificación y transformación del campo, así como la seguridad ciudadana, la justicia y la democracia para la consolidación de la Paz como valor constitucional y el desarrollo ambiental sostenible.

16. Estimular, apoyar y acompañar la incubación, creación y desarrollo de empresas productivas a través de la aplicación de diferentes herramientas administrativas como capacitación, asesoría técnica, otorgamiento de incentivos y demás aspectos que le permitan incidir en la potencialización de la vocación productiva del departamento.

17. Realizar aportes y participar en la creación de sociedades o personas jurídicas de derecho público o privado, alianzas estratégicas, contratos de riesgos compartidos y similares cuya finalidad sea desarrollar proyectos de inversión.

18. Invertir los excedentes de tesorería con fines de rentabilidad social e institucional, y dentro de las políticas establecidas por el Consejo Directivo.

19. Realizar Inversiones patrimoniales en proyectos en ejecución y entes jurídicos existentes que procuren el fomento y desarrollo económico de la región.

20. Celebrar y realizar toda clase de contratos, convenios y operaciones con entidades públicas o privadas dedicadas a la actividad financiera, mediante las cuales se permita la gestión de los recursos entregados en administración a través de la colocación de préstamos a interés y con garantías; a empresas de economía mixtas, privadas o personas naturales con el fin de promover el desarrollo económico y productivo de la región, en el marco del plan de desarrollo departamental.

**Parágrafo.** La selección del tercero deberá cumplir los lineamientos establecidos en el manual de crédito de la entidad, y deberá contar con la experiencia, idoneidad y vigilancia por parte de la Superintendencia correspondiente.

21. Celebrar y realizar toda clase de contratos, convenios, operaciones y, en general, cualquier otra actuación que demande el ejercicio de sus derechos o el cumplimiento que, legal y

contractualmente, se deriven de su existencia y funcionamiento, además que en todo momento le permitan el cumplimiento cabal de su objeto.

22. Constituir, administrar o participar a título oneroso en fondos especiales y/o fondos cuenta con o sin personería jurídica cuyos recursos tengan como destinación la realización de proyectos, financiación de programas de educación de pregrado y postgrado, planes o programas en cumplimiento de su objeto y las funciones y actividades que constituyen éste.

23. Administrar eventual y transitoriamente, obras y/o empresas cuando por razón de los contratos celebrados, se requiera para preservar sus intereses y participar transitoriamente en estas últimas, cuando las condiciones así lo exijan.

24. Adquirir, administrar, enajenar, gravar, arrendar y limitar el derecho de dominio de bienes de toda naturaleza, cuando fuere necesario o conveniente a sus fines, asegurando el mantenimiento y velando por la seguridad de los bienes de su propiedad.

25. Aceptar auxilios, donaciones y asignaciones testamentarias que entidades o personas naturales o jurídicas, privadas, nacionales o internacionales, otorguen para la realización de obras o inversiones de desarrollo para el Departamento, previa verificación del origen legal de los mismos.

26. De igual forma son parte del objeto del Instituto todos los actos jurídicos, actividades y operaciones que deba ejecutar para el cumplimiento de las funciones enlistadas.

**Parágrafo 1.** Los servicios del Instituto serán remunerados en todos los casos con el pago de las comisiones, tasas, tarifas, derechos, honorarios y demás emolumentos cuyos parámetros serán fijados por el Consejo Directivo, de acuerdo con las condiciones del mercado, conforme con criterios racionales y sobre bases contables, excluyendo de esta situación el cumplimiento de un deber legal de la administración central Departamental o el de sus entidades descentralizadas, siempre y cuando se garantice la estabilidad financiera y patrimonial del Instituto.

**Parágrafo 2.** Todas aquellas actividades que se adelanten por parte del instituto en el ámbito regional, podrán ser ejecutadas siempre y cuando se evidencie la existencia de un beneficio directo para el Departamento.

## TITULO II
## DEFINICIONES

**Artículo 6. Definiciones técnicas.** A continuación, se dan las definiciones de los términos técnicos usados en este documento.

**Administración del Plan de Continuidad de Negocios:** Es un sistema administrativo integrado, transversal a toda la organización, que permite mantener alineados y vigentes todas las iniciativas, estrategias, planes de respuesta y demás componentes y actores de la continuidad del negocio.

Busca mantener la viabilidad antes, durante y después de una interrupción de cualquier tipo. Abarca las personas, procesos de negocios, tecnología e infraestructura.

**Administración del Riesgo**. Forma de abordar un problema desde un punto de vista gerencial para disminuir los riesgos inherentes a todo desarrollo de sistemas.

**Amenaza**. Persona, situación o evento natural del entorno (externo o interno) que es visto como una fuente de peligro, catástrofe o interrupción. Ejemplos: inundación, incendio, robo de datos.

**Análisis de Riesgos**. Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos (riesgos) positivos y/o negativos y el impacto de los mismos, calificándolos y evaluándolos a fin de determinar la capacidad de la Entidad para su aceptación y manejo.

**Attachments**. Archivos adjuntos a los mensajes de correo electrónico.

**Causa**. Son los medios, circunstancias y agentes que generan los riesgos. Los agentes generadores son todos los sujetos u objetos que tienen la capacidad de originar un riesgo, como: personas, materiales, instalaciones y entorno. Es el por qué se origina el riesgo.

**Consecuencia**. Constituye los efectos de la materialización del riesgo sobre los objetivos de la entidad. Generalmente se dan sobre las personas y/o los bienes materiales o inmateriales con incidencias importantes como: daños físicos, sanciones, pérdidas económicas, pérdidas de información, de bienes, interrupción del servicio y daño ambiental.

**Control**. Aspectos críticos que se deben tener en cuenta durante la ejecución del proceso o subproceso para atender los resultados.

**Disponibilidad**. Característica, atributo o condición de la información, los datos y los sistemas, de estar a disposición para quienes tengan autorización para su uso, en el momento que sea requerido.

**Dominio: (en inglés domain)**. Sinónimo de dirección de una página principal (homepage) en Internet. El término dominio se usa asimismo para referirse a la identificación de uno o varios servidores conectados a la Red. La asignación de dominios está regulada por el llamado DNS (Domain Name System = Sistema de Nombres de Dominio).

**Dispositivo extraíble:** hace referencia a cualquier dispositivo que se pueda conectar temporalmente a la computadora: una memoria USB (disco flash), una tarjeta de memoria, un disco duro externo, una cámara, un CD, etc.

**Firewall**. Es un dispositivo que asegura las comunicaciones entre usuarios de una red e Internet.

**Gestión de Riesgos**. Es la implementación homologada y sistémica de un conjunto de acciones tendientes al manejo óptimo de los riesgos en todos los procesos, siguiendo el Modelo Estándar de Control Interno – MECI – 2014.

**Identificación del Riesgo**. Elemento de control que posibilita conocer los eventos potenciales, estén o no bajo el control de la Entidad Pública, que pone en riesgo el logro de su Misión, estableciendo los agentes generadores, causas y efectos de su ocurrencia.

**Incidente de Trabajo**. Es un evento que no hace parte de la operación normal de un servicio y el cual puede causar interrupción o reducción en la calidad del servicio y en la productividad.

**Mapa de Riesgos**. La herramienta conceptual y metodológica para la valoración y categorización de los riesgos presentes dentro de la organización.

**Problema de Continuidad de Negocio**. Es un evento interno o externo que interrumpe uno o más de los procesos de negocio. El tiempo de la interrupción determina que una situación sea un incidente o un desastre.

**Plan de Contingencia y Continuidad de Negocio (PCN).** Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios de contingencia y recuperación para retornar y continuar la operación, en caso de interrupción.

**Plan de Recuperación de Desastres (DRP).** Es la estrategia que se sigue para restablecer los servicios de tecnología (red, servidores, hardware y software) después de haber sufrido una afectación por un incidente o catástrofe de cualquier tipo, el cual atente contra la continuidad del negocio.

**Recursos**. Son las cualidades y activos fundamentales con que cuenta una entidad para cumplir con sus objetivos, los cuales deben ser protegidos mediante la Gestión de Riesgos.

**Riesgo**. Es un evento cuya posibilidad de ocurrencia y consecuencias afectan los recursos y objetivos de la Entidad.

**Riesgo Natural o Inherente**. Cualquier incertidumbre o amenaza que pudiera afectar el logro de los objetivos estratégicos de la entidad o afectar el logro de los objetivos del proceso.

**Sistemas de información**. Conjunto de recursos humanos y tecnológicos utilizados para la generación de información, orientada a soportar de manera más eficiente la gestión de operaciones en la Entidad Pública.

**Valoración del Riesgo**. Elemento de control, que determina el nivel o grado de exposición de la organización al impacto del riesgo, permitiendo estimar las prioridades para su tratamiento.

**Vulnerabilidad**. Es una debilidad que se ejecuta accidental o intencionalmente y puede ser causada por la falta de controles, llegando a permitir que la amenaza ocurra y afecte los intereses de la Institución.

## TITULO III
## PROPÓSITO Y ALCANCE

**Artículo 7. Propósito.** Este plan detalla las políticas de Seguridad de la Información del Instituto de Desarrollo de Arauca (IDEAR), el cual sirve como guía formal para la definición, consolidación e implementación de medidas de seguridad y protección de la información, los elementos tecnológicos y las personas que hacen parte del instituto, contribuyendo a proteger y conservar la integridad, confidencialidad y disponibilidad de los datos dentro de los sistemas, procesos y servicios del IDEAR, enfocados en las redes, las instalaciones de cómputo, manejo de la información y procedimientos tecnológicos tanto manuales, como digitales. Se presenta como base de trabajo, con espacio de mejoramiento continuo tanto en los procesos, como en las actividades y procedimientos definidos.

Cualquier problema que sea detectado por las diferentes áreas y usuarios del Instituto que hagan uso de las tecnologías informáticas y comunicaciones en materia de seguridad informática, se deberá informar al área de tecnología de la entidad, como responsable del control y gestión de la seguridad de la información, quien tratará de subsanar lo ocurrido.

**Artículo 8. Alcance.** El Plan de Seguridad Informática del IDEAR, busca proteger la información y los elementos clave dentro del instituto (activos, equipos e infraestructura tecnológica), definiendo las responsabilidades que deben asumir cada uno de los funcionarios de la entidad, durante su permanencia en la misma. Esto con el fin de desarrollar operaciones y servicios seguros, basados en normativas y estándares en seguridad de la información, para que sean divulgados y conocidos por todos los funcionarios de la entidad. Igualmente, se contempla la definición de estrategias y actividades que se deben llevar a cabo durante la implementación de este plan y su permanente control, validación y actualización.

Estas políticas son aplicables a todo el contexto empresarial del IDEAR, incluyendo sus recursos tecnológicos y humanos, a la totalidad de los procesos internos y externos, a los proveedores, prestadores de servicios y/o terceros que de alguna forma pudieran tener alguna manera habitual u ocasional de interacción con la información o con los equipos y dispositivos propios y/o de la entidad. Dentro del alcance e importancia del presente Plan de Seguridad Informática del IDEAR se encuentra:

a) Evaluar los riesgos en seguridad de la información a los que se está expuesta la entidad.
b) Selección de controles y eventos de gestión, para mitigar, eliminar y/o evitar los riesgos identificados.
c) Definir políticas de seguridad, normas y procedimientos, que pautan las actividades relacionadas con la seguridad informática y la tecnología de la información en toda la entidad.
d) Concienciar a todos los funcionarios de la entidad acerca de la importancia de un adecuado manejo de la información y los datos, además de los servicios críticos bien ejecutados por todas las áreas del IDEAR.

e) Comprometer activamente a la entidad en el cumplimiento de las políticas aquí definidas
f) Análisis de la necesidad de cambios o adaptaciones para cubrir los riesgos existentes.
g) Identificar fallas y deficiencias, en pro de renovar y mantener actualizadas estas políticas en función de un mejor ambiente empresarial.

## TITULO IV
## SEGURIDAD DE LA INFORMACIÓN

**Artículo 9. Objetivo del Plan de Seguridad de la Información.** Establecer las políticas relacionadas con la seguridad de la información que, junto con las normas, lineamientos, procedimientos y actividades que hacen parte de los procesos tecnológicos de la entidad, constituyen el cuerpo normativo para la seguridad de información del IDEAR, siguiendo los estándares relacionados a la gestión informática y cumpliendo las regulaciones vigentes.

Las políticas, normas y procedimientos han sido establecidos con el fin de garantizar:

- La confidencialidad de la información.
- La integridad de la información
- La disponibilidad de la información.
- La autenticidad de la información.

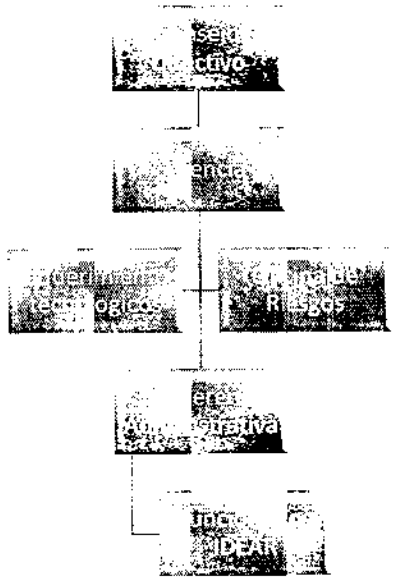
**Artículo 10. Responsables del cumplimiento.** Todo el personal integrante del IDEAR, además de aquellas personas o entidades vinculadas a la entidad, que interactúan de manera habitual u ocasional con los activos de información, son responsables de informarse del contenido del cuerpo normativo de seguridad de información, cumplirlo y hacerlo cumplir en el desarrollo de sus actividades laborales.

Estas políticas de seguridad de la información son de aplicabilidad a todo el personal del Instituto, indistintamente su vinculación al mismo, al área a la cual se encuentre laborando o el nivel de tareas que desempeñe.

El incumplimiento de las políticas de seguridad de información tendrá como resultado la aplicación de diversas sanciones legales, penales y disciplinarias, conforme a su magnitud y características.

**Artículo 11. Organización de la seguridad.** En la administración de la seguridad de la información participan todos los funcionarios del IDEAR. Dentro de la gestión y control de la seguridad informática de la entidad, como apoyo a las demás áreas y con base en el volumen de las operaciones y la criticidad de la información manejada al interior del instituto, se define al responsable del área de tecnología como punto central en Seguridad de la Información, en cabeza del profesional universitario encargado de tecnología del IDEAR y del Jefe de Dficina de Riesgos.

En busca de garantizar un adecuado ejercicio de los procesos y funciones referentes a la seguridad informática del instituto; se adopta una estructura para el análisis, control y prevención tecnológica, constituida de la siguiente forma.



Dentro de las responsabilidades del área de tecnología se encuentra la gestión del plan de seguridad de información, así como la coordinación de esfuerzos entre el líder del área de tecnología y el personal de la institución, siendo estos últimos los responsables de la información que utilizan, sujeto a las políticas, normas y procedimientos definidas en el presente documento.

**Artículo 12. Responsabilidades del Comité de Requerimientos Tecnológicos y Seguridad de la Información.**

a) Establecer y documentar las responsabilidades de la organización en cuanto a la seguridad informática.
b) Mantener las políticas y estándares de seguridad en la información en el IDEAR, monitoreando su cumplimiento por parte de todos los interesados en la entidad.
c) Mantener Actualizado el manual de seguridad informática, de acuerdo a los lineamientos de los entes de control.
d) Identificar objetivos de seguridad, tales como prevención de virus, uso de herramientas de monitoreo etc.
e) Definir metodologías y procesos relacionados con la seguridad informática.
f) Evaluar aspectos de seguridad de productos de tecnología, sistemas o aplicaciones utilizados en el IDEAR.

**Artículo 13. Responsabilidades del Área de Tecnología.** Como líder y punto de referencia en la gestión de las políticas de seguridad informática, el encargado del área de tecnología tiene la responsabilidad de:

a) Identificar objetivos de seguridad, tales como prevención de virus, uso de herramientas de monitoreo etc.
b) Definir metodologías y procesos relacionados con la seguridad informática.
c) Comunicar aspectos básicos de seguridad de información a los funcionarios del IDEAR. Esto incluye un programa de concientización para comunicar aspectos básicos y las políticas, siguiendo los planes de capacitación definidos en la entidad.
d) Controlar e investigar incidentes de seguridad o violaciones de seguridad, previo, durante y posterior a que suceda.
e) Realizar una evaluación periódica de vulnerabilidades de los sistemas conformados por la red de datos del IDEAR.
f) Evaluar aspectos de seguridad de productos de tecnología, sistemas o aplicaciones utilizados en el IDEAR.
g) Verificar que cada activo de información tecnológico del IDEAR haya sido asignado a un propietario, el cual debe seguir los requerimientos de seguridad tales como políticas de protección, perfiles de acceso, respuesta ante incidentes y sea el responsable final del mismo.
h) Coordinar todas las funciones relacionadas a seguridad tales como: seguridad física, seguridad de personal y seguridad de información almacenada en medios no electrónicos.
i) Generar reportes al comité de Requerimientos Tecnológicos y Seguridad de la Información del instituto sobre consolidado de incidentes, informes, validación de información y/o actualización de las políticas en seguridad informática.
j) Administrar los accesos a las principales aplicaciones del IDEAR.

**Artículo 14. Responsabilidades de la Oficina de Riesgos.**

a) Verificar la aplicación del manual de Seguridad de la información y la matriz de riesgos Tecnológicos y de Gestión Documental.
b) Definir metodologías y procesos relacionados con minimizar el riesgo en la seguridad informática.
c) Realizar seguimiento a los eventos de seguridad de la información y las medidas correctivas realizadas por el área de tecnología.
d) Investigar incidentes de seguridad o violaciones de seguridad, previo, durante y posterior a que suceda.
e) Realizar una evaluación periódica de vulnerabilidades de los sistemas conformados por la red de datos del IDEAR.
f) Evaluar controles o aspectos de seguridad de productos de tecnología implementados por el área de tecnología.

**Artículo 15. Responsabilidades de los Usuarios.** Las responsabilidades de los usuarios finales, es decir, aquellas personas que utilizan la información y los medios de comunicación, distribución y transporte de datos del IDEAR como parte de su trabajo son:

a) Mantener la confidencialidad de las contraseñas, haciendo uso adecuado de las mismas (Ver Sección Manejo de Contraseñas).
b) Reportar supuestas violaciones de la seguridad de la información.
c) Asegurarse de ingresar información adecuada a los sistemas de información del instituto, siguiendo los procedimientos para dichas actividades correctamente y no cambiar/modificar/copiar/eliminar (integridad de la información) dichos datos, para beneficio propio y/o de terceros.
d) Adecuarse a las políticas de seguridad del IDEAR.
e) Utilizar la información digital y física de la entidad únicamente para los propósitos autorizados, siguiendo el Código de Ética y los valores corporativos del instituto.
f) Seguir los protocolos y políticas de seguridad informática definidos en el presente plan y apoyados con los demás planes incluidos dentro de los requerimientos tecnológicos de la entidad (Ver Plan de Contingencia y Continuidad del negocio y anexos, ver Plan de Adquisición de Tecnología e Infraestructura y anexos).

**Artículo 16. Acceso a terceros.** Los proveedores, contratistas externos y demás personas y/u organizaciones vinculadas al IDEAR deben cumplir con las responsabilidades y seguir los lineamientos definidos para los funcionarios del Instituto. Igualmente, el acceso a la información debe limitarse a lo mínimo indispensable para cumplir con el trabajo asignado, siguiendo los acuerdos y actividades definidos dentro de los contratos vinculantes con el instituto, manteniendo la confidencialidad de la información involucrada en sus procesos y cumpliendo a cabalidad con el servicio prestado/ofrecido.

Las excepciones o casos especiales deben ser presentados ante la Gerencia, la subgerencia administrativa y/o el área de tecnología, encargados de analizar, aprobar y/o rechazar dichas solicitudes, incluyendo aquellos referentes a los accesos físicos o gestión de datos lógicos de los recursos de información del Instituto. Igualmente, los terceros seguirán los procedimientos referentes al incumplimiento y violación de la seguridad de la información, definidos para los funcionarios del IDEAR.

**Artículo 17. Fuerza de seguridad.** El sistema de seguridad del Instituto está compuesto por un sistema abierto de 8 cámaras de vigilancia, las cuales son monitoreadas desde el área de tecnología, con conexión por internet a Gerencia.

a) Frente del Instituto. Panorámica.
b) Entrada de primero piso, detrás de correspondencia.
c) Vista panorámica de la Subgerencia Comercial y de Cartera, Subgerencia Administrativa, Talento Humano y Presupuesto.
d) Vista panorámica de la Subgerencia Financiera, Tesorería y Almacén.
e) Vista panorámica del archivo.
f) Vista panorámica interna segundo piso.
g) Vista panorámica interna tercer piso.
h) Vista panorámica al área del servidor.

La seguridad nocturna del Instituto depende de las cámaras de vigilancias y el apoyo de un profesional en vigilancia a partir de las 6:00 p.m. hasta las 5:00 a.m. resguardado en el interior del primer piso con la puerta cerrada con llave, monitoreando constantemente el exterior y la puerta del acceso al segundo piso se cierra con candados y cadenas. Además, es una zona muy transitada por los cuadrantes de la policía, al estar el comando de policía a tres cuadras.

Igualmente, se deben tener en cuenta los siguientes lineamientos, por parte del personal de vigilancia, visitantes y funcionarios de la entidad:

a) El ingreso a una persona a las áreas restringidas será solo con el debido acompañamiento en todo momento de la persona responsable del área.
b) Se debe notificar a la persona encargada en la recepción del instituto de la salida definitiva de las instalaciones, para hacer una revisión a sus elementos personales y el debido registro y verificación a elementos que vayan a ser retirados del instituto.
c) Todos los empleados deben tener especial cuidado de no permitir el paso a personas no autorizadas a áreas restringidas.
d) Todo equipo informático sea propio o de terceros que procese información o posea alguna conectividad con los sistemas del IDEAR, debe cumplir con normas de seguridad física que eviten el acceso a los mismos de personas no autorizadas, los computadores, equipos de comunicación, teléfonos, no deben moverse reubicarse o ser sacados de las instalaciones sin realizar el procedimiento de autorización adecuado ante el área de tecnología, la Gerencia del IDEAR y/o el área encargada de la gestión de dichos elementos.

## TITULO V
## RIESGOS

**Artículo 18. Evaluación de riesgos.** Como parte del proceso de definición y categorización de los procedimientos de seguridad de la información del IDEAR, además de obtener un adecuado entendimiento de la importancia que tiene el uso de la tecnología e identificación de las amenazas y vulnerabilidades a los que está expuesta la entidad, se realiza la evaluación de riesgos del instituto.

Este proceso se consolida por medio del documento MATRIZ DE RIESGOS TECNOLÓGICOS – IDEAR. Dentro de dicha matriz, se categorizan los elementos propios asociados a la tecnología de la entidad (activos, riesgos, vulnerabilidades, impacto, amenazas y salvaguardas). Con esta lista de elementos identificados, se clasifican en eventos según su trascendencia dentro de la seguridad del instituto (dinámico físico, dinámico organizativo y estático). Finalmente, se definen 4 subprocesos en donde se involucran los elementos analizados, que son: análisis del riesgo, planificación, gestión de riesgos y selección de salvaguardas.

Esta evaluación de riesgos permite al área de tecnología y en general, a todos los funcionarios y el contexto empresarial del IDEAR a:

a) Tener una herramienta de categorización de los riesgos tecnológicos presentes en la entidad, enfatizada en las vulnerabilidades tecnológicas de la misma.
b) Llevar a cabo planes de seguridad informática y de contingencia adecuadamente.
c) Identificar claramente las fuentes de posibles riesgos y vulnerabilidades de los elementos físicos y tecnológicos de la entidad.
d) Definir procedimientos de mitigación de riesgos tecnológicos y aplicarlos en el momento en que sea requerido.
e) Concienciar tanto a los responsables del manejo de la información dentro de la entidad, como a los demás funcionarios, a conocer la existencia de posibles riesgos tecnológicos y la necesidad de enfrentarlos a tiempo.

**Artículo 19. Análisis de Riesgos Tecnológicos**. Los propietarios de la información y custodios son conjuntamente responsables del desarrollo de análisis de riesgo tecnológico anual de los sistemas a su cargo, Como parte de este análisis, se deben identificar las aplicaciones de alta criticidad para la recuperación ante eventualidades tecnológicas. Para esto, es importante identificar:

a) Áreas Vulnerables.
b) Pérdida potencial.
c) Selección de controles y objetivos de control para mitigar los riesgos indicando las razones para su inclusión o exclusión, (Seguridad de datos, plan de respaldo/recuperación, procedimientos de operación).

Adicionalmente, un análisis de riesgo tecnológico debe ser ejecutado, luego de cualquier cambio significativo en los sistemas de información de la entidad, en concordancia con los cambios que se generen de las operaciones y procesos del Instituto. Este análisis debe tener un propósito claramente definido y delimitado, existiendo dos posibilidades: Cumplimiento con los controles y/o medidas de protección o la aceptación del riesgo (Ver Anexo MATRIZ DE RIESGOS TECNOLÓGICOS – IDEAR).

**Artículo 20. Cumplimiento**. El cumplimiento satisfactorio del proceso de evaluación del riesgo y su aplicación dentro del contexto empresarial del IDEAR se caracterizan por:

a) Identificación y clasificación correcta de los activos a ser protegidos.
b) Aplicación consciente y continua de medidas para mitigar el riesgo (seguridad efectiva de datos, recuperación ante desastres)
c) Detección temprana de los riesgos, reporte adecuado de pérdidas, así como una respuesta oportuna y efectiva ante las pérdidas ya materializadas.

Una vez realizado este proceso y su posterior verificación, se deben cumplir las políticas definidas en el mismo por parte de todos los funcionarios de la entidad, aplicando los controles de riesgo definidos y mantener una constante actualización de los mismos.

**Artículo 21. Aceptación de Riesgos**. La Gerencia, la subgerencia administrativa y/o el área de tecnología, pueden obviar algún control o requerimiento de protección y aceptar el riesgo identificado

sólo cuando ha sido claramente demostrado que las opciones disponibles para lograr el cumplimiento han sido verificadas, comprobadas y que estas no tendrían un impacto significativo y no aceptable para el instituto.

La aceptación del riesgo por falta de cumplimiento de los controles y/o medidas de protección debe ser documentada, revisado por las partes involucradas, comunicada por escrito y aceptada por el área de tecnología y/o la gerencia del instituto.

## TITULO VI
## ACTIVOS

**Artículo 22. Inventario de activos.** Los inventarios de activos ayudan a garantizar la vigencia de una protección eficaz de los recursos, al igual que pueden ser necesarios para otros propósitos empresariales (Ver SISTEMA INFORMATICO IDEAR), además de los identificados en la MATRIZ DE RIESGOS TECNOLÓGICOS – IDEAR.

## TITULO VII
## CLASIFICACIÓN DE ACCESO A LA INFORMACIÓN

**Artículo 23. Clasificación de acceso A la información.** Con el fin de mantener autenticidad, confidencialidad, integridad y disponibilidad de los datos digitales y los elementos físicos que hacen parte de la infraestructura tecnológica y están involucrados en los procesos del IDEAR, se debe clasificar la información, según su tipo, nivel de privacidad y contenido. Por tanto, se define el siguiente esquema para el proceso de clasificación de la información:

**Restringida**. Aquella información privilegiada en donde su divulgación no autorizada puede derivar en impactos financieros, legales, con la ciudadanía, con proveedores, con el propio gobierno y/o entidades externas. Ejemplos: datos de adquisiciones (antes de su anuncio), negociaciones, desarrollo de nuevos servicios, juicios, etc.

**Confidencial**. Aquella en donde su divulgación no autorizada puede derivar en impactos importantes para la operación de la Dependencia, perdiendo principalmente la oportunidad. Ejemplos: Información sobre operaciones y transacciones del Instituto, resoluciones y actas de comités, información de clientes, nómina y compensaciones, contraseñas, entre otras.

**Privada**. Es aquella información ordinaria del Instituto que apoya sus procesos internos y que no ha sido clasificada como restringida ni confidencial, por lo que puede ser conocida dentro de toda la organización. No puede ser difundida a clientes ni a terceros. Su divulgación no autorizada representa un impacto menor para el Instituto. Ejemplo: directorio telefónico personal de los funcionarios, comunicados internos.

**Pública**. Es la información que ha sido autorizada expresamente para darse a conocer al público en general a través de canales aprobados. Ejemplo: propaganda, boletines de prensa, páginas de Internet, estados financieros, manuales de procedimientos, presupuestos, reportes de auditoria, etc.

La clasificación asignada a la información solo puede ser cambiada por el funcionario, luego de justificar formalmente el cambio ante su jefe inmediato, el área de tecnología, la Gerencia y/o Consejo Directivo, el (los) cual(es) debe(n) analizar y validar. Igualmente, debe ser examinada para determinar el impacto para el IDEAR, si fuera divulgada o alterada por medios no autorizados.

Frecuentemente, la información deja de ser sensible después de un cierto periodo de tiempo, este aspecto debe ser tomado en cuenta por el propietario para realizar una reclasificación. Dicho periodo debe ser de al menos 6 meses, a partir de su formalización dentro del almacenamiento de documentos de la entidad o al momento de su reclasificación.

A continuación, se encuentran documentos o similares, que pueden contener información sensible o que puede estar sujeta a posibles vulnerabilidades:

**Datos de interés para la competencia.**

a) Estrategias de mercadeo.
b) Lista de clientes.
c) Fechas de renovación de créditos
d) Tasas
e) Datos usados en decisiones de inversión (llaves de autenticación, contraseñas).

**Datos protegidos por legislación de privacidad vigente.**

a) Registros del personal.
b) Montos de los pasivos de clientes.
c) Datos históricos con 10 años de antigüedad.

**Datos que tienen un alto riesgo de ser blanco de fraude u otra actividad similar.**

a) Datos contables utilizados en los sistemas.
b) Sistemas que controlan desembolsos de fondos.
c) Datos de autenticación a bancos.

**Artículo 24. Aplicación de controles para La información clasificada.** Mantener un control y gestión adecuada de la información clasificada dentro del IDEAR, es esencial para mantener el nivel de confidencialidad adecuado y garantizar un permanente nivel de seguridad óptimo en los procesos de la entidad. Las medidas de seguridad aplicadas a los activos de información clasificada incluyen, pero no se limitan a las siguientes categorías de información:

**Artículo 25. Información almacenada en forma digital.** Toda información catalogada como digital es aquella que se encuentra almacenada o guardada en los discos duros o elementos electrónicos disponibles en el instituto (CD's, cintas magnéticas, USB's, etc.). Dicha información puede haber sido digitalizada (escaneada, fotografiada) de su archivo físico, transferida vía correo electrónico o a través de otros mecanismos de digitalización y envío de información. Estos formatos digitales

incluyen documentos realizados por medio de programas de edición de texto (Word, Excel, Bloc de Notas y similares), de edición de presentaciones (Power Point) o aplicativos de creación de documentos digitales.

A continuación, se presentan las políticas de seguridad relacionadas con la información digital del IDEAR y sus elementos de almacenamiento:

a) La información en formato digital clasificada como PÚBLICA puede ser almacenada en cualquier sistema del instituto y se deben tomar las medidas necesarias para no mezclarla con otra clasificación.

b) Todo usuario antes de transmitir información clasificada como RESTRINGIDA O CONFIDENCIAL, debe asegurarse que el destinatario de la información este autorizado para recibir dicha información.

c) Todo usuario que requiera acceso a la información clasificada como RESTINGIDA O CONFIDENCIAL, debe ser autorizado por el propietario de la misma y, por tanto, deben ser documentadas.

d) La información en formato digital clasificada como RESTRINGIDA debe ser encriptada por un método aprobado por los administradores de la seguridad cuando es almacenada en cualquier medio.

e) Toda transmisión de información clasificada como RESTRINGIDA, CONFIDENCIAL o PRIVADA realizada desde redes externas del Instituto, debe realizarse utilizando un medio de transmisión seguro o utilizando técnicas de encriptación probadas.

f) Todo documento en formato digital debe presentar la clasificación correspondiente en la parte superior (encabezado) e inferior (pie de página) de cada página del documento o como marca de agua, al fondo de cada página.

g) Los medios de almacenamiento, incluyendo discos duros de computadoras que albergan información clasificada como RESTRINGIDA, deben ser ubicados en ambientes cerrados diseñados para el almacenamiento de dicho tipo de información. Es decir, un lugar que garantice protección física y de seguridad (bajo llave).

h) Todo contenedor de la información en medio digital debe presentar una etiqueta con la clasificación correspondiente

**Artículo 26. Información almacenada en formato no digital.** La información catalogada como no digital es aquella que se encuentra en formato físico (papel y otro material similar) y es almacenada en el archivo de la entidad y/o en los archivos de los funcionarios del IDEAR. Las políticas de seguridad referentes a la información no digital del instituto son:

a) Todo documento o contenedor de información RESTRINGIDA, CONFIDENCIAL, PRIVADA O PÚBLICA debe ser etiqueta de acuerdo a la clasificación asignada.

b) Todo documento que presente información clasificada como RESTRINGIDA o CONFIDENCIAL debe ser etiquetada en la parte superior e inferior de cada página según corresponda.

c) Todo documento clasificado como RESTRINGIDA o CONFIDENCIAL debe presentar una caratula que muestre la clasificación a que corresponde.

d) El ambiente donde se almacena la información clasificada como RESTRINGIDA, debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia, el acceso solo será para personal formalmente autorizado.

e) Solo el personal formalmente autorizado debe tener acceso a información clasificada como RESTRINGIDA o CONFIDENCIAL.

f) Los usuarios que utilizan documentos con información RESTRINGIDA o CONFIDENCIAL deben asegurarse de:

1. Almacenarlos en lugares adecuados.
2. Evitar que usuarios no autorizados accedan a dichos documentos.
3. Destruir los documentos si, luego de su utilización, dejan de ser necesarios (Ver Tablas de Retención Documental).

**Artículo 27. Reproducción y copia de la información.** Sobre la copia o reproducción de la información y los datos del IDEAR, se estipula lo siguiente:

a) Reportes confidenciales y restringidos no deben ser copiados, sin la autorización del propietario de la información.

b) Reportes e información confidencial solo pueden ser copiados para los funcionarios autorizados a conocer su contenido. La Gerencia, la subgerencia administrativa y el director del área respectiva son los responsables de determinar dicha necesidad, para la persona a la cual le sea distribuido dicho reporte.

c) Los reportes e información restringida deben ser controlada por un solo custodio (director del área respectiva, área de tecnología), quien es responsable de registrar las personas autorizadas a utilizar la información.

d) La copia de cualquier información o dato restringido o confidencial almacenado en un medio magnético y físico debe ser aprobado por el propietario, el área de tecnologia o la Gerencia del instituto y debe ser clasificado igual que el original.

e) La única área autorizada para realizar dicha reproducción o copia de la información digital es el ÁREA DE TECNOLOGIA, con previa autorización, seguimiento y control por parte de la Gerencia y la subdirección administrativa del instituto.

**Artículo 28. Distribución de la información.** La información clasificada como CONFIDENCIAL y RESTRINGIDA debe ser controlada cuando es transmitida por correo electrónico corporativo (Ver Sección INTERCAMBIOS DE INFORMACIÓN Y CORREO ELECTRÓNICO), correo externo o postal. Tanto en la distribución de información por correo electrónico, como la hecha por el servicio postal, se debe solicitar una confirmación de entrega al receptor.

Los reportes confidenciales y otros documentos sensibles deben usarse en conjunto con sobres confidenciales sellados. La entrega personal es requisito indispensable para la información extremadamente sensible.

Todo usuario, antes de transmitir información clasificada como RESTRINGIDA o CONFIDENCIAL, debe asegurarse que el destinatario de la información esté autorizado a recibir dicha información.

La transmisión e intercambio de información clasificada como RESTRINGIDA o CDNFIDENCIAL hecha desde y/o hacia el IDEAR, debe realizarse utilizando un medio de transmisión seguro. Es recomendable el uso de técnicas de encriptación para dicha información transmitida, además de documentar el registro de este proceso, detallando fecha y hora del envío y/o recepción.

**Artículo 29. Eliminación de la información.** La eliminación de documentos y otras formas de información debe asegurar la confidencialidad de la información de las unidades de negocio involucradas y/o que puedan verse afectadas con este proceso.

Previo a la eliminación final, se debe realizar la copia de respaldo de la información contenida en los discos duros, las cintas magnéticas, USB's, CD's, etc., que se dejen de usar en el instituto, debido a daño u otro factor, antes de que éstos sean destruidos. Luego, se procede a borrar la información en dichos dispositivos y finalmente hacer la adecuada destrucción del dispositivo y la correcta eliminación de la información (Ver Plan de Adquisición de Tecnología e Infraestructura, Sección Gestión de Cambio de Equipos y Elementos Tecnológicos).

## TITULO VIII
## SEGURIDAD DEL PERSONAL

**Artículo 30. Seguridad del personal.** Los estándares de seguridad relacionados al personal y los funcionarios del IDEAR deben ser aplicados para asegurarse que los nuevos empleados sean seleccionados adecuadamente antes de ser contratados. De igual forma, pueden ser fácilmente identificados mientras formen parte de la entidad y que el acceso será revocado oportunamente cuando un empleado es despedido o transferido (Ver Manual de Funciones IDEAR).

Los funcionarios son los activos más valiosos dentro del IDEAR. Como los otros elementos tecnológicos, no están exentos de vulnerabilidades y amenazas, referentes a la seguridad de la

información que se procesan durante su labor diaria y que pueden perjudicar el normal funcionamiento del instituto. Por tanto, cada funcionario debe seguir e implementar los procedimientos para la identificación y manejo de los riesgos y ayudar al personal de la entidad a crear un ambiente adecuado y seguro de trabajo.

Se deben tomar medidas de precaución cuando se hace la contratación, despido o transferencia de alguno de los funcionarios de la entidad. Se deben seguir los protocolos establecidos en el área respectiva para cada uno de los procesos enunciados anteriormente, apoyado con controles de comunicación en cambios de personal y requerimientos de elementos tecnológicos al área de TECNOLOGIA. Estos cambios deben ser atendidos en el menor tiempo posible. Igualmente, se debe realizar el procedimiento de eliminación de usuarios dentro de los sistemas de información del instituto, asegurando que la información manejada por cada uno de ellos quede respaldada dentro de las copias de seguridad de la entidad y sus datos de identificación sean eliminados correctamente.

Esta política de seguridad del personal debe ser aplicada a todas las personas, como los empleados de planta, contratistas y proveedores.

**Artículo 31. Seguridad en la definición de puestos de trabajo y recursos**. Con respecto a la seguridad en los puestos de trabajo y recursos dispuestos en el IDEAR, se debe tener en cuenta lo siguiente:

a. Cualquier elemento tecnológico o electrónico entregado al funcionario tales como: portátil, computador de escritorio, tabletas, celulares, memorias USB, llaves digitales, software, datos, documentación, manuales, etc., deben ser entregados a su jefe inmediato o al área de tecnología. Debe quedar registro de los elementos entregados, fecha y firma de recibido.

b. La seguridad es responsabilidad de todos los funcionarios, contratistas, proveedores y demás personas involucradas en el día a día del IDEAR. Por tanto, todas las personas deben acatar las políticas y normas de seguridad física, de infraestructura y de la información definidas para la entidad, priorizando la seguridad en sus labores corporativas, extendiéndolas a su vida personal y profesional.

c. Los equipos que sean utilizados por los funcionarios de la entidad, que no son propiedad de los mismos y son adicionales a los que se encuentran disponibles en las instalaciones del instituto, deben seguir las políticas en confidencialidad y seguridad de la información definidas para los equipos de la entidad y deben tener un control, aprobación y vigilancia por parte del área de tecnología y/o la Gerencia del IDEAR. (Un computador para la entidad SOLAMENTE).

d. Los funcionarios deben seguir las políticas, normas de seguridad y lineamientos del área respectiva, conscientes de todas sus responsabilidades y acciones apropiadas en el reporte de incidentes y manejo de la información del instituto.

**Nota aclaratoria**. Referente a los equipos de cómputo, portátiles, tabletas y/u otros dispositivos que sean de propiedad de los funcionarios y sean utilizados para el manejo de información del instituto (creación, edición, eliminación de datos), para las labores diarias en sus áreas y/o utilización de los aplicativos financieros y demás disponibles en la entidad, se establece lo siguiente:

e. La utilización de estos equipos por parte de los funcionarios y contratistas como herramienta de trabajo, hace que estos equipos sean adoptados por la entidad. Por tanto, el área de tecnología debe hacer el seguimiento, mantenimiento y soporte técnico aplicado a los equipos propios del instituto. Igualmente, se deben instalar los programas y aplicativos utilizados tanto para la gestión de información, como aquellos de seguimiento y auditoria, además de la integración a la red de la entidad.

f. Dada la adopción del equipo por parte del instituto, éste debe permanecer dentro de las instalaciones del instituto. Si requiere ser retirado, se debe presentar la solicitud al área de tecnología y la gerencia y/o la subdirección administrativa, detallando el tiempo que durará el equipo fuera de las instalaciones, el nombre del funcionario/contratista que se lo lleva, fecha de salida y la descripción u objetivo de la necesidad de utilizar el equipo externamente. El funcionario debe reportar el retorno del equipo a las instalaciones directamente al área de tecnología.

g. Dada la adopción del equipo por parte del instituto, dichos equipos deben contener únicamente y sin excepción información corporativa. Está prohibido el manejo de la información personal del funcionario, contratista u otra persona en dichos equipos.

h. Aquellos equipos adoptados (e identificados por el área de tecnología como tal) por la entidad, que presenten algún tipo de información personal de funcionarios, contratistas y/o archivos o datos que no sean parte del instituto y sus procesos, se definirán como de propiedad del funcionario. Por tanto, no se podrá manejar información del instituto ni utilizar los aplicativos dispuestos por el IDEAR para la labor diaria de sus empleados.

i. En caso de que alguno de estos equipos adoptados (e identificados por el área de tecnología como tal) contenga información tanto del instituto, como personal del funcionario/contratista o externa a los datos y procesos de la entidad, se definirán como de propiedad del funcionario. Por tanto, no serán sujetos a mantenimiento, soporte o asistencia técnica por parte del instituto. Estos servicios serán asumidos por el funcionario/contratista, dueño del equipo.

j. El área de tecnología no está en la obligación de realizar algún procedimiento sobre dichos equipos adoptados, si se comprueba que contiene información externa al instituto.

k. El área de tecnología está en la obligación de reportar a la gerencia y a la subgerencia administrativa cualquier irregularidad con dichos equipos y de llevar registro, seguimiento y control de los mismos.

l. En caso de que el funcionario/contratista se desvincule del instituto por cualquier motivo y haya dado uno o varios equipos en adopción al IDEAR, el área de tecnología debe:

1) Realizar copia de seguridad de la información del instituto contenida en el(los) equipos adoptados.
2) Eliminar tanto la información ya copiada y almacenada, tanto como los aplicativos y demás programas del instituto instalados en el mismo.
3) Desvincular el(los) equipo(s) de la red de datos, asegurando que cualquier dato y/o conexión sea eliminada adecuadamente.
4) Entregar el(los) equipo(s) adoptado(s) al funcionario, guardando registro del número de serie y demás datos de identificación el(los) equipo(s).

**Artículo 32. Seguridad en dispositivos móviles.** El IDEAR proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos, inteligentes y tabletas, entre otros) institucionales y personales que hagan uso de servicios del instituto. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por la entidad:

a. La seguridad es responsabilidad de todos los funcionarios, contratistas, proveedores y demás personas involucradas en el día a día del IDEAR. Por tanto, todas las personas deben acatar las políticas y normas de seguridad física, de infraestructura y de la información definidas para la entidad, priorizando la seguridad en sus labores corporativas, extendiéndolas a su vida personal y profesional.

b. El área de Requerimientos Tecnológicos debe investigar y probar las opciones de protección de los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por el instituto.

c. El área de Requerimientos Tecnológicos debe establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por el IDEAR.

d. El área de Requerimientos Tecnológicos debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.

e. El área de Requerimientos Tecnológicos debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.

f. El área de Requerimientos Tecnológicos debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de

eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

g. El área de Requerimientos Tecnológicos debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales del IDEAR; dichas copias deben acogerse a la Política de Copias de Respaldo de la Información.

h. El área de Requerimientos Tecnológicos debe configurar los dispositivos móviles institucionales con la cuenta institucional del usuario responsable del dispositivo.

i. El área de Requerimientos Tecnológicos debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

j. Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

k. Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.

l. Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.

m. Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.

n. Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth o infrarrojos en los dispositivos móviles institucionales asignados.

o. Los usuarios no deben hacer uso de los dispositivos móviles para compartir internet por ningún medio a otros dispositivos.

p. Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

q. Los usuarios no deben almacenar vídeos, fotografías o información personal en los dispositivos móviles institucionales asignados.

r. Los usuarios no deben registrar cuentas de correo electrónico personales en dispositivos que sean propiedad del IDEAR

**Artículo 33. Capacitación de usuarios.** Es responsabilidad del Área de Tecnología y la Gerencia del Instituto promover constantemente la importancia de la seguridad a todos los usuarios de los sistemas de información del IDEAR. El programa de concientización en seguridad debe contener continuas capacitaciones, charlas y campañas de divulgación. Adicionalmente, se puede emplear diversos métodos como afiches, folletos informativos y/o correos electrónicos para divulgar la información, los cuales permiten recordar permanentemente a los funcionarios e interesados el papel importante que cumplen en el mantenimiento, seguimiento y actualización de la seguridad de la información en el instituto, sus responsabilidades y aportes en este sentido. Dentro de dichas capacitaciones se debe incluir al menos lo siguiente:

a. Identificador de usuario y contraseña, así como su correcta gestión y uso.
b. Seguridad del puesto y equipo de trabajo, incluyendo la protección de virus, manejo de sesiones de usuario y bloqueo de computadores.
c. Responsabilidades en la organización de la seguridad de la información.
d. Recomendaciones y alertas sobre ataques informáticos, malware, spam, etc.
e. Programas de cumplimiento e implementación en seguridad informática.
f. Guías de acceso, manejo y uso del correo electrónico e internet.
g. Procesos de monitoreo y control de la seguridad de la información utilizados.
h. Persona(s) de contacto para información adicional y apoyo.
i. Difusión de las políticas de equipos y la información de la entidad.
j. Planes, brigadas y manejo de emergencias (Ver Plan de Contingencia y Continuidad del Negocio – IDEAR).

Como apoyo a las capacitaciones y demás actividades realizadas y buscando incrementar considerablemente la retención y conocimiento acerca de la importancia de la seguridad de la información en el IDEAR, se debe informar con una periodicidad de máximo un año las políticas de seguridad informática a todos los funcionarios de la entidad. Esto, por medio de las actividades descritas anteriormente, apoyadas con un resumen de las medidas básicas e información referente a la seguridad, el cual el funcionario debe tener siempre a disposición.

**Artículo 34. Procedimientos para nuevos funcionarios y/o servicios con terceros.** Al momento de contratar un nuevo funcionario o un servicio con una persona externa al Instituto, se le debe hacer entrega de las políticas de seguridad de la información, así como las normas, lineamientos y procedimientos para el uso de las aplicaciones y los sistemas de información de la entidad. Igualmente, los proveedores deben adjuntar los Planes de Contingencia de los respectivos servicios que ofrece al Instituto. Además, se debe hacer entrega de un resumen escrito, con las medidas básicas de seguridad de la información del IDEAR.

Junto con la documentación anterior, el personal referente al servicio externo (tercero), debe recibir una copia del acuerdo de no divulgación aprobado y firmado por la gerencia del Instituto y el proveedor del servicio, incluyendo la responsabilidad de ambas partes en la confidencialidad de la información que se maneje durante la prestación del servicio. De igual manera, se debe tener en cuenta:

a. El personal de la entidad y que brinda el servicio debe ser comunicado de las medidas de seguridad relacionadas a las responsabilidades del trabajo a ejecutar.
b. Se debe guardar una copia firmada de las políticas de seguridad de la información, por parte del funcionario que recibe el servicio y del personal externo que lo ofrece.
c. Todos los procedimientos y actividades que sean realizadas por el proveedor del servicio, deben ser monitoreadas y con el debido seguimiento por parte del líder del área donde se esté desarrollando la actividad. Esto, con previa autorización de la gerencia, reportando cada actividad al término de esta.

## TITULO IX
## INCIDENTES DE SEGURIDAD

**Artículo 35. Procedimientos de respuesta ante incidentes de seguridad.** Con respecto a los procedimientos de respuesta ante incidente de seguridad, se define lo siguiente:

a. El líder del área de tecnología, como encargado de la administración de la seguridad informática del IDEAR, debe ser plenamente identificado por el personal e interesados de la entidad.

b. Si algún funcionario del IDEAR detecta o sospecha la ocurrencia de un incidente de seguridad, tiene la obligación de reportarlo y notificarlo al área de tecnología o a la Gerencia del instituto.

c. Si se sospecha la presencia de un virus o malware en uno o varios de los sistemas, aplicativos o documentos digitales de la entidad, el funcionario o usuario debe desconectar el equipo de la red de datos y notificar inmediatamente al área de tecnología, para iniciar proceso de eliminación del virus. Es responsabilidad del funcionario (con la apropiada asistencia técnica) asegurarse que el virus haya sido eliminado completamente del sistema antes de reactivarse el sistema y de conectarse de nuevo a la red de datos de la entidad. El funcionario no debe proceder a realizar ninguna acción, sin la supervisión del área de tecnología.

d. Si un funcionario, durante el desarrollo de su labor diaria, detecta que el sistema de seguridad presenta algún tipo de vulnerabilidad o amenaza, debe reportarlo inmediatamente al área de tecnología y/o a la Gerencia del instituto. Igualmente, está prohibido que el empleado de la entidad realice pruebas sobre esta posible vulnerabilidad, así tenga el conocimiento para ello, incluyendo la posibilidad que pueda aprovechar dicha vulnerabilidad para beneficio propio o de terceros.

e. Es responsabilidad del área encargada de la seguridad informática (área de tecnología), documentar todos los reportes de incidentes de seguridad.

f. Cualquier error, bloqueo inesperado o falla en alguno de los sistemas y aplicativos de la entidad, debe ser notificado al área de tecnología, la cual determinará el procedimiento a seguir y su posible impacto dentro de la seguridad de la información del Instituto.

g. En caso de la ocurrencia de alguna violación de seguridad (robo de información, infiltración de datos, etc.), se deben aplicar acciones disciplinarias acordes con la magnitud de la falta, apoyado con el área de talento humano, el área jurídica y/o la Gerencia del instituto. Posterior a esto y como base procesal del incidente en seguridad, el gerente será el responsable de dar inicio, seguimiento y finalización de la investigación o proceso legal a que haya lugar, velando para que a la persona involucrada en la falta se le realice el debido proceso, con todas las garantías legales y disciplinarias vigentes.

**Artículo 36. Las acciones disciplinarias tienen la siguiente categorización.**

a) **Falta leve**. Referente a situaciones de seguridad de la información, que no tengan impacto sobre los procesos de la entidad, pero que puedan generar vulnerabilidad sobre los sistemas de información y la infraestructura de la entidad, tales como: transmitir información no verídica entre los funcionarios de la entidad, compartir los correos corporativos personales con otras personas, utilizar dichos correos para temas ajenos a la organización, ausentarse de las instalaciones sin autorización, etc. En estos casos, se deben aplicar acciones definidas para los funcionarios, según los parámetros establecidos en el código de ética de la entidad y/o similares. En este caso, se debe realizar un llamado de atención a él(los) funcionario(s) de manera verbal y escrita, con anotación en su bitácora de trabajo, hoja de vida o similar.

b) **Falta moderada.** Aquellas situaciones en donde se involucre información privada del instituto, ya sea por infiltración a la misma, copia no autorizada, adulteración de los datos o alguna actividad similar, que impacte levemente al instituto o alguno de los componentes de la infraestructura de la entidad (funcionarios, equipos, aplicativos). Se deben aplicar medidas disciplinarias como: suspensión por uno a dos días al funcionario y/o personas involucradas, memorandos y compromisos ante el Instituto.

c) **Falta grave.** Situación en donde se presenta robo, alteración, modificación, eliminación u otro tipo de actividades que impactan directamente los procesos del instituto y su infraestructura. Se entran a tomar medidas disciplinarias, acorde con la falta que se haya cometido, entre las cuales se deben incluir: suspensión del funcionario durante el tiempo que dure la investigación, retiro del funcionario amonestación escrita en la hoja de vida y demás procedimientos penales y legales que sean concernientes a la magnitud de la falta.

**Artículo 37. Registros de fallas.** El personal encargado de operar los sistemas de información (Área de Tecnología) debe registrar todos los errores y fallas que ocurren en el procesamiento,

manejo y gestión de la información o en los sistemas de comunicaciones. Estos registros deben incluir lo siguiente:

a) Nombre de la persona que reporta la falla.
b) Hora y fecha de la ocurrencia de la falla.
c) Descripción del error o problemas.
d) Responsable de solucionar el problema.
e) Descripción de la respuesta inicial ante el problema.
f) Descripción de la solución del problema.
g) Hora y fecha en que se solucionó el problema.

Los registros de fallas deben ser revisados semanalmente. Los registros de errores no solucionados deben permanecer abiertos hasta que se encuentre una solución del problema, Además, estos registros deben ser almacenados para una posterior verificación independiente (Ver Anexo – Formato de Registro de Fallas – IDEAR).

**Artículo 38. Administración de incidentes de seguridad.** Al momento de presentarse algún incidente de seguridad del instituto, que haya sido identificado por el funcionario o personal de la entidad, se debe seguir el procedimiento a continuación:

a) Una vez reportado el incidente de seguridad, éste es investigado por el área de tecnología, encargada de la seguridad informática del IDEAR. Se identifica la severidad del incidente para la toma de medidas correctivas.
b) El área de tecnología, apoyado con la subgerencia administrativa y/o la gerencia del instituto, realiza la investigación correspondiente de (los) incidente(s) de forma rápida y confidencial.
c) El instituto debe tener una documentación permanente de todos los incidentes de seguridad ocurridos, detallando el procedimiento ejecutado para su control, por medio del área de tecnología.
d) Se debe mantener intacta la evidencia y/o las pruebas recopiladas durante el registro del incidente, que prueba la ocurrencia de una violación de seguridad producida tanto por entes internos o externos, para su posterior utilización en procesos legales en caso de ser requerido.

## TITULO X
## SEGURIDAD DE DATOS

**Artículo 39. Intercambios de información y correo electrónico.** Los mensajes gestionados por medio del correo electrónico corporativo del IDEAR son considerados como datos e información formal de la entidad, los cuales hacen parte de registro de datos de la entidad y están sujetas a monitoreo y auditoria. Los sistemas de correo electrónico no deben ser usados para lo siguiente:

a) Enviar cadenas de mensajes.
b) Enviar mensajes relacionados a seguridad, exceptuando al personal encargado de esta en la entidad.

c) Enviar propaganda de candidatos políticos.
d) Actividades ilegales, no éticas e impropias.
e) Actividades no relacionadas con las funciones de políticas de calidad y responsabilidades del IDEAR.

**Parágrafo 1.** No deben utilizarse reglas de reenvió automático a direcciones que no pertenecen al IDEAR. No se puede tener control sobre los correos electrónicos, una vez estos se encuentren fuera de la red de la entidad.

**Parágrafo 2.** Al momento de iniciar un proceso con un proveedor o tercero, se deben establecer controles sobre el intercambio de información, asegurando la confidencialidad e integridad de la misma, respetando la propiedad intelectual y los acuerdos establecidos previo a la ejecución de la actividad. Se debe tener en cuenta:

a) Acuerdos para el intercambio de software.
b) Seguridad en forma de tránsito de la información.
c) Controles sobre la transmisión mediante redes o conexiones remotas.
d) Planes de Contingencia de los servicios ofrecidos.

**Parágrafo 3.** La información contenida en la página web del instituto o en sistemas públicos no debe contener datos restringidos, confidenciales, privados o de uso interno de la entidad. Igualmente, los equipos que brindan servicios web, correo electrónico o servicios afines no deben almacenar información catalogada como restringida, confidencial o privada. Antes de la divulgación de información no pública por parte de algún funcionario de la entidad, se debe verificar su identidad dentro del IDEAR y del receptor de la información, ya sea por medio de la identificación personal, referencias de terceros, registro de comunicación entre las partes o mecanismos similares que permitan comprobar su identidad.

**Parágrafo 4.** Los equipos dentro de las instalaciones del IDEAR como teléfonos, impresoras, conmutadores, etc., que procesen información sensible de la entidad, deben tener controles de seguridad, verificados por el área de tecnología y seguir las políticas y procedimientos establecidos en este documento. Igualmente, información restringida, confidencial, pública y/o de manejo interno del instituto, debe imprimirse en los equipos autorizados y designados específicamente para esta tarea.

**Artículo 40. Seguridad para los datos en tránsito.** La información a ser transferida en forma digital o impresa debe ser etiquetada con la clasificación de información respectiva, detallando claramente el remitente y a la persona a la que va dirigida. La información enviada por servicios de correo certificado debe ser protegida de accesos no autorizados mediante la utilización de:

a) Paquete sellado
b) Entrega en persona
c) Firmado y sellado por la compañía de correspondencia.

**Artículo 41. Seguridad física de las instalaciones de procesamiento de datos.** El IDEAR implementa medidas de seguridad física, con el fin de asegurar la integridad de las instalaciones. Las medidas de protección son acordes con al nivel de clasificación de los activos y el valor de la información procesada y almacenada en el Instituto. (Ver Plan de Contingencia y Continuidad del Negocio - IDEAR).

**Artículo 42. Protección de las instalaciones de los centros de datos.** El centro de procesamiento de datos o de cómputo se define como el edificio contenedor de equipos de almacenamiento, procesos o transmisión de información, es decir abarca el conjunto de las instalaciones del Instituto, que incluye:

a) Servidores, computadoras personales y periféricos.
b) Equipos de telecomunicaciones.
c) Centrales telefónicas, PBX.
d) Armarios de cableado.

Para el caso del IDEAR, este centro de procesamiento se refiere a las instalaciones de la entidad, se encuentra ubicada en la ciudad de Arauca, en la calle 15 # 13 - 46.

Los controles son evaluados anualmente por el Gerente, la Subgerencia Administrativa y el Área de Tecnología. Esto, para compensar cualquier cambio con relación a los riesgos físicos y el diseño de los controles físicos de seguridad de la entidad.

**Artículo 43. Control de acceso a las instalaciones de cómputo.** El acceso a cualquier instalación de cómputo está restringido únicamente al personal autorizado. El IDEAR, dentro de sus medidas de control de acceso a las instalaciones de cómputo, mantiene un registro escrito que permite la identificación de las visitas a dichas instalaciones, reflejando fechas y horas exactas de ingreso y salida como también actuaciones realizadas.

Como medida de control de acceso físico, el IDEAR establece el uso restringido de llaves, las cuales están bajo la responsabilidad del área de tecnología del Instituto, encargada de aumentar la protección de los bienes protegidos, tales como: caja fuerte para almacenamiento de las copias de seguridad, cuarto de servidores, etc.

Se debe tener un adecuado registro e identificación del personal que ingrese a realizar algún tipo de actuación en los equipos de cómputo, de la misma manera se deberá hacer el acompañamiento al personal autorizado en el transcurso del desarrollo de las actividades. El retiro de cualquier equipo o medio electrónico de las instalaciones de cómputo debe ser aprobado por escrito por el área de tecnología de la entidad.

**Artículo 44. Protección contra Malware.** Los sistemas de información del IDEAR, como programas o aplicativos existentes, esta propenso a amenazas informáticas permanentemente. Por tanto, es esencial que el Área de Tecnología, tome medidas preventivas y correctivas referentes a este tipo de amenazas. El antivirus con el que cuenta la entidad es Kaspersky Internet Security 2016 multidispositivo por un término de 2 años con vencimiento en febrero de 2019.

Cualquier equipo de un tercero que se deba conectar a la red, debe contener su respectivo antivirus, previa revisión del Área de Tecnología.

**Artículo 45. Copias de respaldo.** Dentro del procedimiento para la realización de copias de respaldo y backups del IDEAR, se incluyen los pasos y actividades para la generación de las copias de respaldo, establecido por el área de tecnología, con la documentación y el detalle del proceso ejecutado. Este procedimiento se encuentra especificado en el PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO DEL IDEAR– Sección Políticas de Copias de Seguridad de Datos.

**Artículo 46. Control de acceso a datos.** La información manejada por los sistemas de información y las redes asociadas al IDEAR debe estar adecuadamente protegida contra modificaciones no autorizadas, divulgación o destrucción. El uso inteligente de controles de acceso previene errores o negligencias del personal, así como reduce la posibilidad del acceso no autorizado.

## TITULO XI
## COMUNICACIONES Y OPERACIONES

**Artículo 47. Administración de comunicaciones y operaciones.** La administración de las comunicaciones y operaciones del IDEAR es importante para ofrecer los servicios a los clientes del instituto adecuadamente. Dichos procedimientos se estipulan en este documento y deben ser soportados por los planes de contingencia y continuidad del negocio y de adquisición de tecnología e infraestructura. Además, de los documentos, formatos y anexos referidos a los mismos. Los cambios realizados a dichos procedimientos deben ser revisados y autorizados por la Gerencia y el Área de Tecnología del Instituto.

Los procedimientos operacionales, las responsabilidades para el manejo y control de acceso a los sistemas de información del instituto, así como la disponibilidad e integridad de los mismos, deben ser incluidos en las funciones operativas de la entidad. Todo intercambio de información y comunicaciones, dentro y fuera del instituto, deben ser aseguradas, de acuerdo al nivel y valor de la información protegida (Ver Sección CLASIFICACIÓN DE ACCESO A LA INFORMACIÓN).

**Artículo 48. Procedimientos y responsabilidades operacionales.** Todos los procedimientos de operación de los sistemas, programas, equipos y aplicativos del IDEAR, deben ser documentados y sus cambios serán revisados y aprobados por la Gerencia, con apoyo de la subgerencia administrativa y el área de tecnología.

A continuación, se presenta el procedimiento básico de encendido y apagado de los equipos de cómputo de la entidad:

a) **Encender el Computador.** Para encender el computador se deben tener en cuenta los siguientes pasos:

1. Los cables de poder deben conectarse a la toma de energía regulada.
2. Se prende el estabilizador, batería, pila o UPS (Sistema ininterrumpido de Potencia), en caso que se tenga disponible en el equipo.
3. Se enciende la CPU, presionando el botón Encender (Power).
4. Se prenden los parlantes, que de acuerdo con la configuración de sonidos que se tenga, permitirá oír cómo se abren y cierran programas hasta llegar a la activación completa del computador (si aplica).
5. Por último, se enciende la pantalla como apoyo visual.

b) **Apagado del Computador.** Para apagar el computador se deben tener en cuenta los siguientes pasos:

1. Debe guardarse la información, previo a cerrar los programas en ejecución y guardar la información.
2. Se activa la ventana de menú de inicio presionando la tecla Windows o se señala con el mouse hacia la derecha del escritorio (Windows 8).
3. Para la versión de Windows 7 o anteriores, o Windows 10, se da clic en el botón de Inicio o símbolo de Windows que se encuentra en la esquina inferior izquierda, dar clic en la opción apagar. En esta lista de opciones también se encuentra: Cerrar sesión de administrador, Reiniciar y Suspender (según versión del Sistema Operativo).
4. Se espera que la CPU se apague normalmente, hasta que se haya apagado la luz de apoyo y su ventilador se haya apagado.
5. Finalmente, se apaga la pantalla, los parlantes y se apaga el estabilizador (si aplica), asegurándose de dejar adecuadamente desconectado el equipo de la toma de energía.
6. Asegurase que el equipo se encuentra totalmente apagado antes de desconectar cables o apagar estabilizadores y para el caso de computadores portátiles antes de cerrarlos.
7. para el caso de computadores portátiles dejar desconectado el cargador.

Este procedimiento también aplica para equipos portátiles de la entidad o los propios de los funcionarios del instituto. Se recomienda trabajar con la conexión a corriente directamente, hasta completar la carga al cien por ciento, posterior a esto se debe desconectar el equipo a la fuente de corriente y trabajar con la batería. Esto para que la pila tenga un mayor tiempo de vida útil.
Todas las tareas programadas en los sistemas para su realización periódica, también son documentadas. En este documento debe incluir tiempo de inicio, tiempo de duración de la tarea, procedimientos en caso de falla, entre otros.

c) **Los procedimientos para resolución de errores deben ser documentados, entre ellos debe incluir.**

1. Errores en la ejecución de procesos por partes
2. Fallas o apagado en los sistemas.
3. Códigos de error en la ejecución de procesos por partes.
4. Información de los contactos que podrían colaborar con la resolución de errores.

**Artículo 49. Administración de operaciones realizadas por terceros.** Todos los procesos de operación realizados por terceros son sujetos a una evaluación de riesgos de seguridad y se deben desarrollar procedimientos para administrar estos riesgos (Ver Anexo Matriz de Riesgos Tecnológicos – IDEAR y Sección PROCEDIMIENTOS PARA NUEVOS FUNCIONARIOS Y/O SERVICIOS CON TERCEROS). Se debe tener en cuenta lo siguiente, al momento de ejecutar procedimientos con terceros:

a) Asignación de responsables para la supervisión de dichas actividades
b) Determinar si se procesará información crítica.
c) Determinar los controles de seguridad a implementar
d) Evaluar el cumplimiento de los estándares de seguridad del instituto.
e) Evaluar la implicancia de dichas tareas en los planes de contingencia del instituto.
f) Procedimientos de respuesta ante incidentes de seguridad
g) Evaluar el cumplimiento de los estándares del instituto referentes a contratos con terceros.

**Artículo 50. Control de Cambios Operacionales.** Los controles y gestión de cambios operacionales, deben seguir las siguientes políticas.

a) Todos los cambios realizados en los sistemas de la entidad, a excepción de los cambios de emergencia, siguen los procedimientos de cambios establecidos.
b) Solo el área de tecnología, con apoyo de la Gerencia, pueden realizar o aprobar un cambio de emergencia. Dicho cambio debe ser documentado y aprobado en un periodo máximo de 24 horas luego de haberse producido.
c) Los roles del personal involucrado en la ejecución de los cambios en los sistemas se encuentran debidamente especificados (Ver Sección ORGANIZACIÓN DE LA SEGURIDAD).
d) Todos los requerimientos de cambios deben ser debidamente documentados, siguiendo los procedimientos para cambios existentes y con la debida aprobación del área de tecnología.
e) Antes de la realización de cualquier cambio a los sistemas se deben generar copias de respaldo de dichos sistemas, las cuales deben ser almacenadas bajo los mismos procedimientos de manejo de copias de seguridad definidos para el Instituto.

**Artículo 51. Separación de funciones de desarrollo y de operaciones.** El IDEAR cuenta con aplicativos y programas adquiridos con proveedores externos en soluciones informáticas financieras. Por tanto, debe seguir las políticas y procedimientos específicos a cada uno de dichos sistemas, manteniendo la autenticidad, confidencialidad, integridad y disponibilidad de la información, los datos y los servicios que ofrecen los mismos. Igualmente, se debe mantener contacto permanente con los proveedores y su personal de soporte técnico, para desarrollar las tareas de adecuación, actualización, cambio y/o demás requerimientos especiales a realizar sobre los aplicativos.

Las funciones operacionales y de desarrollo (de software) del instituto, deben seguir las siguientes políticas:

a) El ambiente de prueba debe mantenerse separado del ambiente de desarrollo, con controles adecuados para cada uno de ellos.

b) Solo el personal autorizado por la entidad y el proveedor del servicio debe contar con privilegios de escritura o cambios en los aplicativos sujetos a modificar. Igualmente, dicho personal solo tiene acceso de solo lectura de la información del Instituto, la cual está sujeta a términos de confidencialidad.

c) Ningún programa compilador o ambiente de desarrollo de software debe ser instalado en los equipos del IDEAR. Cualquier código debe ser previamente compilado antes de ser transferido e instalado en los equipos del Instituto.

d) parágrafo: Se Exceptúa de esta condición los equipos del área de tecnología, que serán utilizados como equipos de prueba para ambiente de desarrollo. estos serán especificados debidamente y al momento de ser utilizados para este trabajo.

e) Las pruebas deben realizarse con datos de prueba. En caso de ser requerido el uso de copias de datos de la entidad, se debe contar con la adecuada autorización del área de tecnología, realizar el debido seguimiento a este manejo y deben ser manejados de manera confidencial. Igualmente, se debe tener control sobre la información que se utiliza en este procedimiento, la cual no deberá alterar ningún dato dentro de dicha información del Instituto.

f) Todo procedimiento ejecutado y tareas de control de cambios deben estar debidamente documentados, revisados y aprobados por el área de tecnología y la gerencia del IDEAR.

## TITULO XII
## CONTROLES, ACCESO Y GESTIÓN DE DATOS

**Artículo 52. Identificación de usuarios.** Las políticas referentes a la identificación de usuarios dentro de los sistemas de información del IDEAR son:

a) Cada usuario debe ser identificado de manera única y el acceso del usuario, así como su actividad en los sistemas debe ser controlado, monitoreado y revisado.

b) Cada usuario de un sistema debe tener un código de identificación que no sea compartido con otros usuarios, para lograr el acceso a los sistemas se requiere que el usuario provea una clave que solo sea conocida por él.

c) Debe ejecutarse el procedimiento para asegurar que el código de identificación de un usuario sea bloqueado de todos los sistemas cuando un empleado es despedido, retirado o transferido; Esta acción deberá realizarse en coordinación con el profesional universitario encargado del proceso de Talento Humano. (notificación)

d) El usuario debe ser instruido en el uso correcto de las características de seguridad y debe cerrar la sesión o bloquear la estación de trabajo cuando se encuentre desatendida.

e) Todos los sistemas deben proveer pistas de auditoría del ingreso a los sistemas y violaciones de los mismos, A partir de estos datos, el encargado del área de tecnología del Instituto debe elaborar reportes periódicos que deben incluir la identidad del usuario, la fecha y la hora del evento. En caso de ser necesario, las violaciones de seguridad deben ser reportadas a la Gerencia del instituto.

f) Las Violaciones repetitivas, significantes o intentos de acceso deben ser reportados a la Gerencia o al área de tecnología.

**Artículo 53. Seguridad de contraseñas.** Las políticas referentes a la seguridad, manejo y administración de las contraseñas son las siguientes:

a) Todas las contraseñas deben tener una longitud mínima de ocho (8) caracteres y no deben contener espacios en blanco.
b) Las contraseñas deben ser difíciles de adivinar, combinando mayúsculas (al menos un carácter), minúsculas (al menos un carácter), números (al menos un carácter) y caracteres especiales (al menos un carácter).
c) Palabras de diccionario, identificadores de usuario y secuencias comunes de caracteres (12345678, ABCDEFG, etc.), deben evitarse. Igualmente,
d) Datos personales como los nombres de familiares, número de documento de identidad, número de teléfono o fechas de cumpleaños no deben ser usadas, salvo acompañados con otros caracteres adicionales que no tengan relación directa.
e) En caso de olvidar la contraseña, debe acercarse al área de tecnología, para su proceso de recuperación.
f) Si sospecha de alguna violación de seguridad en su contraseña o intrusión a su equipo de cómputo, debe reportarlo inmediatamente al área de tecnología y/o la Gerencia, para verificar e iniciar el proceso correspondiente. (Debe quedar en el plan anticorrupción).

**Vigencia.** Con referencia a la vigencia de las contraseñas, éstas deben expirar dentro de un periodo que no exceda los noventa (90) días calendario. El periodo de vigencia de las contraseñas para

todos los funcionarios de la entidad será determinado por la Gerencia del instituto. El mínimo recomendable es de treinta (30) días calendario.

Referente a este tema en especial, el área de tecnología debe hacer recordatorios periódicos a los funcionarios de la entidad, divulgando información acerca de las políticas de uso de las contraseñas y el cambio que deben hacer de la misma. Para esto, se debe manejar un periodo entre 30 a 60 días calendario, con comunicación vía correo electrónico y/o mensajes informativos.

**Artículo 54. Reutilización de contraseñas.** Para todos los funcionarios de la entidad:

a) No debe permitirse la reutilización de ninguna de las 4 últimas contraseñas definidas por cada uno de ellos. Esto asegura que los usuarios no utilicen las mismas contraseñas en intervalos regulares.
b) Los usuarios no deben poder cambiar sus contraseñas más de una vez al día. En caso tal, se debe identificar esta irregularidad y comunicarse lo más pronto posible con el funcionario.
c) Los usuarios con privilegios de administrador y/o súper usuarios, no deben poder reutilizar o reasignar su nueva contraseña con alguna de las 10 previamente definidas.

**Artículo 55. Intentos fallidos de ingreso.** Todos los sistemas deben estar configurados para deshabilitar los identificadores de los usuarios en caso de ocurrir (3) intentos fallidos de autenticación. En caso de que ocurra esta situación, el funcionario debe comunicarse con el área de tecnología, para seguir el procedimiento correspondiente de recuperación de su contraseña.

Si alguno de los aplicativos o programas utilizados o que se vayan a instalar en los equipos de cómputo del IDEAR no cuentan con características de utilización de contraseñas y no se puedan aplicar las políticas definidas sobre ellas, se debe documentar esta situación, detallando la viabilidad de la adecuación del aplicativo para el uso de contraseñas.

**Artículo 56. Manejo de contraseñas.** Es importante que todos los funcionarios del IDEAR sean conscientes de su responsabilidad en el manejo de sus contraseñas. Para esto, deben seguir las siguientes especificaciones:

a) Bajo ninguna circunstancia se debe escribir las contraseñas en papel o almacenarlas en medios digitales no encriptados.
b) Las contraseñas no deben ser divulgadas a ningún otro usuario, salvo bajo el pedido de la Gerencia, con autorización del área de tecnología de la entidad. Si se divulga la contraseña, esta debe ser cambiada durante el próximo ingreso.
c) El usuario autorizado es responsable de todas las acciones realizadas por alguna persona a quién se le ha comunicado la contraseña o identificador de usuario.
d) Los sistemas no deben mostrar la contraseña en pantalla o en impresiones, para prevenir que éstas sean observadas.

e) El control de acceso a archivos, bases de datos, computadoras y otros sistemas de recursos mediante contraseñas compartidas está prohibido.

**Artículo 57. Control de transacciones.** Todos los funcionarios del instituto están sujetos a controles sobre sus procesos y transacciones de información (interacción con los servicios del sistema financiero y los demás aplicativos que intervienen en procedimientos financieros), durante su labor diaria. Por tanto, deben seguir las siguientes normas, referentes a la gestión de las transacciones realizadas:

a) Los funcionarios deben tener acceso únicamente al conjunto de transacciones en línea requeridas para ejecutar sus tareas asignadas. Este conjunto de transacciones debe estar claramente definido para prevenir alguna ocurrencia de fraude y malversación.
b) El conjunto de transacciones (perfiles de usuario) debe ser definido durante el proceso de desarrollo de sistemas, revisado periódicamente y gestionado por el encargado del área de tecnología, con la verificación y aprobación de la Gerencia y/o la subgerencia administrativa del instituto.
c) El acceso para la ejecución de transacciones sensibles debe ser controlado mediante una adecuada segregación de tareas. Para el caso, los usuarios que tengan permiso para registrar instrucciones de pago no deben poder verificar o aprobar su propio trabajo.
d) Toda operación realizada en los sistemas que afecten información sensible como saldos contables, deben contar con controles duales de aprobación. Dichos controles de aprobación deben ser asignados con una adecuada segregación de funciones.
e) Reportes de auditoría de transacciones sensibles o de alto valor deben ser revisados por la gerencia. Estos reportes deben incluir la identidad del usuario, la fecha y la hora del evento.

**Artículo 58. Control de acceso a programas.** Los controles de acceso de programas deben asegurar que los usuarios no puedan acceder a la información sin autorización. Por tanto, los aplicativos contenidos en el sistema de información del IDEAR deben cumplir con lo siguiente:

a) Los programas deben generar una pista de auditoría de todos los accesos y violaciones.
b) Las violaciones de los controles de acceso deben ser registradas, revisadas y verificadas por el área de tecnología, como administrador de la seguridad informática del instituto.
c) Las violaciones de seguridad deben ser reportadas a la Gerencia y al área de tecnología del instituto.
d) Se debe tener cuidado particular en todos los ambientes, asegurando que ninguna persona tenga control absoluto. Por ejemplo, los operadores de sistemas no deben tener acceso ilimitado a los identificadores de súper usuario. Dichos identificadores de usuario, son solo necesarios durante una emergencia y deben ser cuidadosamente controlados por la Gerencia, apoyada por el área de tecnología, quien debe realizar un monitoreo periódico de su utilización.

**Artículo 59. Administración de acceso a usuarios.**

a) La asignación de identificadores de usuarios especiales o privilegiados (como cuentas administrativas y supervisores) debe ser revisada cada 3 meses. Es recomendable realizar revisiones trimestralmente debido al continuo cambio de los ambientes de trabajo y la importancia de los datos.
b) El encargado del área de tecnología y/o el propietario de la información gestionada en los sistemas de información del instituto, son responsables de revisar los privilegios de los sistemas periódicamente y de retirar todos aquellos que ya no sean requeridos o utilizados por los usuarios finales.
c) Es responsabilidad de la Gerencia del IDEAR, con el acompañamiento del área de tecnología, ver que los privilegios de acceso estén alineados con las necesidades del instituto. Verificar que dichos privilegios sean asignados basándose en requerimientos y que se comunique la lista correcta de accesos al área de tecnología de información.
d) En las situaciones donde los usuarios con accesos a información altamente sensible sean despedidos o retirados de su cargo, se debe ejecutar la eliminación de sus privilegios y de acceso de ese usuario, por parte del área de tecnología. Igualmente, se debe revisar y/o verificar cualquier archivo físico o digital creado y/o modificado por el funcionario, asignando la propiedad de dicha información a la persona interesada en la misma y determinando la destrucción de archivos innecesarios, con previa verificación de importancia y copia de respaldo correspondiente.
e) Se debe buscar el desarrollo de soluciones técnicas para evitar el uso de accesos privilegiados innecesarios.
f) Todos los usuarios que tienen acceso a las cuentas privilegiadas deben tener sus propias cuentas corporativas personales para uso del negocio. Por ende, los administradores y funcionarios con acceso a cuentas privilegiadas deben usar sus cuentas personales para realizar actividades de tipo no privilegiadas.
g) Cuentas de usuario que no son utilizadas por noventa (90) días deben ser identificadas y ser deshabilitadas automáticamente. Las cuentas que no han sido utilizadas por un periodo largo demuestran que el acceso de información de ese sistema no es necesario. Igualmente, el área de tecnología debe informar periódicamente a la Gerencia o la subgerencia administrativa la existencia de las cuentas inactivas.
h) Todos los accesos a los sistemas de información deben estar controlados a través de un método de autenticación, incluyendo una combinación mínima de identificador de usuario/contraseña. Dicha combinación debe proveer la verificación de la identidad del usuario.
i) Todos los usuarios de los sistemas de información deben tener un identificador de usuario único, que sea válido durante su periodo laboral. Este identificador de usuario no debe de ser utilizado por otras personas, incluso luego de que el usuario original ya no se encuentre activo en los sistemas de información del instituto.

j) Los sistemas no deben permitir que los usuarios puedan tener sesiones múltiples para un mismo sistema, salvo bajo autorización específica de la Gerencia o el área de tecnología y para el desarrollo de tareas o actividades específicas, para beneficio del instituto.

**Artículo 60. Responsabilidades del usuario.** Como usuarios permanentes de los programas y aplicativos incluidos en el sistema de información del instituto, los funcionarios y el personal del IDEAR tienen las siguientes responsabilidades:

a. Todo equipo de cómputo, alquilado o de propiedad del IDEAR, será utilizado solo para actividades relacionadas con los procesos y servicios del Instituto.
b. Los aplicativos y programas del instituto no pueden ser usados para desarrollar software para negocios personales o externos a él.
c. Los equipos no deben ser usados para preparar documentos para uso externo, salvo bajo el previo conocimiento y/o la aprobación escrita de la Gerencia o el área de tecnología del instituto.
d. Se deben implementar protectores de pantallas en todas las computadoras personales y servidores, activándose luego de cinco (5) minutos de inactividad. Igualmente, se deben establecer fondos de escritorio con imágenes alusivas al instituto, tales como: logo corporativo, comunicaciones, boletines informativos, etc.
e. Toda actividad realizada utilizando el identificador de usuario asignado, es responsabilidad del funcionario a quién le fue definido. Por consiguiente, los usuarios no deben compartir la información de su identificador con otros o permitir que otras personas utilicen su identificador de usuario para realizar cualquier acción.
f. Para evitar conexiones externas peligrosas, ciberataques o descargar de programas maliciosos, se hace indispensable el bloqueo de páginas de dudosa procedencia o que no cumplan con normatividad de seguridad, en caso de ser necesario el ingreso a alguna página bloqueada este debe ser con previa autorización de la Gerencia, la subgerencia administrativa y/o el área de tecnología.
g. El uso de dispositivos extraíbles en los equipos del instituto, propios o adoptados, se hace con previa autorización de la Gerencia, la subgerencia administrativa y/o el área de tecnología, para evitar la filtración de información o software malicioso.
h. Para todos los usuarios, está prohibido realizar cualquier acción utilizando un identificador que no sea el propio.
i. Cada funcionario de la entidad es responsable de la información que administra en su equipo de cómputo.
j. Es prohibido el consumo de bebidas y alimentos en los lugares de trabajo, cerca de los equipos de cómputo.

**Artículo 61. Seguridad de computadores.** Las políticas sobre la seguridad de los equipos de cómputo del instituto son:

a. Se debe mantener un inventario actualizado de todo el software y hardware existente en el IDEAR. La responsabilidad del mantenimiento y gestión de dichos elementos es del área de tecnología del instituto.

b. Todo traslado o asignación de equipos debe ser requerida por el área de tecnología y debe ser aprobada por la Gerencia del instituto. Es responsabilidad del encargado del área de tecnología la verificación y realización del requerimiento correspondiente.

c. Es responsabilidad del funcionario, personal del instituto o usuario final, efectuar un correcto uso del equipo de cómputo que le fue asignado, así como de los programas en instalados en el mismo. Cualquier cambio y/o traslado deberá ser solicitado con la debida anticipación a la Gerencia o al área de tecnología del instituto. Asimismo, el usuario debe verificar que cualquier cambio y/o traslado del Equipo de Cómputo que le fue asignado, se realice por personal de Soporte Técnico, así como también la instalación o retiro de software del mismo.

d. Cualquier computador personal, portátil o dispositivo móvil perteneciente al IDEAR debe ser únicamente utilizado para propósitos corporativos, de negocios y de servicios de la entidad, tales como:

    1) Terminal de comunicación con otro dispositivo.
    2) Computador aislado que realice su propio procesamiento, sin comunicación con ninguna otra computadora.

e. Sin importar su uso, las medidas de seguridad deben ser implementadas en todos los dispositivos y computadores de la entidad.

f. Una vez habilitada la computadora, ésta no debe dejarse desatendida, incluso por un periodo corto. Para esto, al momento de dejar el puesto de trabajo, cada funcionario debe bloquear el equipo, a través del cierre de sesión (tecla Windows + L o desde el botón de inicio) y apagar la pantalla del equipo. Si es portátil, debe ser configurado para que cuando se cierre la pantalla, se bloquee y no se apague.

g. Todas las cintas, CD's y otros dispositivos de almacenamiento de información incluyendo información impresa, que contengan datos sensibles deben ser guardados en un ambiente seguro cuando no sean utilizados (Ver Plan de Contingencia y Continuidad del Negocio IDEAR – Sección Políticas de Copias de Seguridad de Datos).

h. El acceso a los datos almacenados en un dispositivo móvil o computador portátil debe ser limitado a los usuarios apropiados.

i. Los discos duros no deben contener datos sensibles, salvo en los computadores cuyo acceso físico sea restringido o que tengan instalados algún programa de seguridad y que los accesos al computador y a sus archivos sean controlados adecuadamente.

j. Deben generarse copias de respaldo de documentos y datos de manera periódica. Asimismo, deben desarrollarse procedimientos para su adecuada restauración en el caso de pérdida (Ver SECCIÓN COPIAS DE RESPALDO).

k. Todos los programas instalados en las computadoras deben ser legales, estar debidamente licenciados, aprobados y periódicamente inventariados.

l. Solo los programas adquiridos o aprobados para ser utilizados en el IDEAR, serán instalados en los equipos de cómputo del Instituto.

m. El uso de programas de juegos, de distribución gratuita (freeware o shareware) o de propiedad personal está prohibido, salvo que éste sea aprobado por la gerencia y se haya revisado la ausencia de virus en el mismo.

**Artículo 62. Control de acceso a redes.** Los sistemas de red son vulnerables y presentan riesgos inherentes a su naturaleza y complejidad. Los accesos remotos (dial-in) y conexiones con redes externas, exponen a los sistemas de información del IDEAR a niveles mayores de riesgo. Asegurando que todos los enlaces de una red cuenten con adecuados niveles de seguridad, se logra que los activos más valiosos de las unidades de negocio estén protegidos de un ataque directo o indirecto. Por tanto, se deben seguir las siguientes indicaciones, referentes al control de acceso a redes del instituto:

a) Todas las conexiones realizadas entre la red interna del IDEAR e Internet, deben ser controladas por un firewall para prevenir accesos no autorizados. El área de tecnología debe aprobar todas las conexiones con redes o dispositivos externos.

b) El acceso desde internet hacia la red interna del IDEAR no debe ser permitido sin un dispositivo con autenticación fuerte o certificado basado en utilización de contraseñas dinámicas. Igualmente, debe estar autorizado y verificado por el área de tecnología del instituto.

c) El esquema de direccionamiento interno de la red no debe ser visible desde redes o equipos externos. Esto evita que "hackers" u otras personas pueden obtener fácilmente información sobre la estructura de red del IDEAR y acceder a los datos de los computadores de la entidad.

d) Para eliminar las vulnerabilidades inherentes, enrutadores y firewalls deben rechazar conexiones externas que parecieran originarias de direcciones internas.

e) Para poder hacer uso de la conexión inalámbrica del instituto, se debe tener autorización por parte del área de tecnología, la cual verificará el dispositivo a conectar e ingresará la contraseña de red, sin divulgarla al funcionario o persona autorizada a conectar. Para esto, se debe diligenciar el formato para la conexión a la red inalámbrica, dispuesta en el Área de Tecnología.

**Artículo 63. Estándares Generales.** Sobre el control de acceso a la red del IDEAR y a sus equipos de cómputo, se siguen los siguientes lineamientos:

a) Los accesos a los recursos de información deben solicitar como mínimo uno de los tres factores de autenticación, los cuales son:

   1) Factor de conocimiento: algo que solo el usuario conoce, como: contraseña o PIN.
   2) Factor de posesión: algo que solo el usuario posee, como: SmartCard o token.
   3) Factor biométrico: algo propio de las características biológicas del usuario, tales como: lectores de huella o identificadores de voz/rostro.

b) Todos los componentes de la red deben mostrar el siguiente mensaje de alerta o similares en el acceso inicial. "Aviso de alerta: Estos sistemas son de uso exclusivo del personal y funcionarios autorizados del IDEAR. El uso no autorizado está prohibido y sujeto a procesos legales vigentes".

c) Todos los componentes de la red de datos deben ser identificados de manera única y su uso debe ser restringido. Esto incluye la protección física de todos los puntos vulnerables de una red.

d) Las estaciones de trabajo y equipos de cómputo personales deben ser bloqueados mediante sistema operativo, mientras se encuentren desatendidas.

e) Todos los dispositivos de red, así como el cableado deben ser ubicado de manera segura.

f) Cualquier unidad de control, servidor y rack de comunicaciones debe estar ubicado adecuadamente, protegido a accesos no autorizados.

**Artículo 64. Políticas del uso de servicio de redes.** Todas las conexiones de red internas y externas deben cumplir con las políticas definidas por el IDEAR sobre servicios de red y control de acceso. Es responsabilidad del área de tecnología determinar lo siguiente:

a) Elementos de la red que pueden ser accedidos.
b) El procedimiento de autorización para la obtención de acceso.
c) Controles para la protección de la red.

Todos los servicios habilitados en los sistemas deben contar con una justificación acorde con las necesidades y requerimientos del IDEAR. Los riesgos asociados a los servicios de red deben determinarse y ser resueltos antes de la implementación del servicio. Algunos servicios estrictamente prohibidos incluyen TFTP e IRC/Chat y similares.

**Artículo 65. Control De Acceso Al Sistema Operativo.** El sistema operativo es el programa instalado en todos los equipos de cómputo, el cual gestiona los recursos de hardware y software del mismo. Por tanto, su correcta utilización y manejo permite que los aplicativos instalados en cada uno de los equipos funcionen adecuadamente, manteniendo un óptimo nivel de los procesos y ofreciendo correctamente los servicios propios del IDEAR. El conocimiento y aplicación de las políticas para su control de acceso son importantes para todos los funcionarios de la entidad.

**1) Estándares generales**

a) Los usuarios que posean privilegios de súper usuario, deben utilizar el mismo identificador con el que se autentican normalmente en los sistemas de información de la entidad.
b) El área de tecnología debe otorgarle los privilegios especiales a los identificadores de los usuarios que lo necesiten.
c) Todos los usuarios deben poseer un único identificador. El uso de identificadores de usuario compartidos debe estar sujeto a autorización, seguimiento y supervisión.
d) Solo debe existir una cuenta de usuario dentro del sistema operativo y debe tener privilegios de administrador.

**2) Limitaciones de horario.** Las aplicaciones críticas deben estar sujetas a periodos de acceso restringidos, el acceso a los sistemas en un horario distinto debe ser deshabilitado o suspendido. Por tanto, el horario habilitado para el uso de los equipos de cómputo del IDEAR es el correspondiente a la jornada laboral establecida por el instituto. Para accesos en horarios diferentes, se debe hacer la solicitud anticipada ante el área de tecnología y la Gerencia del instituto, especificando la razón por la cual se hará este uso extra, las actividades a realizar y el horario estipulado para dicho proceso.

**3) Administración de contraseñas.** El área de tecnología, como administradora de seguridad informática, debe realizar pruebas mensuales sobre la calidad de las contraseñas que son empleadas por los usuarios. Todas las bases de datos o aplicaciones que almacenen contraseñas deben ser aseguradas, de tal manera que solo el administrador de los sistemas tenga acceso a ellas. (Ver Sección Seguridad de Contraseñas).

**4) Inactividad del sistema.**

a) Las sesiones en los equipos y sistemas operativos que se encuentren inactivas o desatendidas por más de 30 minutos, deben ser concluidas de manera automática.

b) Los computadores personales y servidores deben ser configurados con un protector de pantalla con contraseña, cuando sea aplicable.
c) El periodo de inactividad para la activación automática del protector de pantalla debe ser de 5 minutos.
d) El sistema operativo debe forzar la reautenticación de los usuarios luego de una (1) hora de inactividad.

**5) Estándares de autenticación en el sistema.**

a) Los sistemas y aplicativos deben mostrar avisos preventivos sobre los accesos no autorizados, durante el proceso de autenticación.
b) Los identificadores de los usuarios deben ser bloqueados luego de 3 intentos fallidos de autenticación en los sistemas. En caso de bloqueo, el funcionario debe comunicarse con el área de sistemas para iniciar el proceso de desbloqueo manual del equipo.
c) Los sistemas deben ser configurados para no mostrar ninguna información que pueda facilitar el acceso a los mismos, luego de intentos fallidos de autenticación (Ver subsección Control de Acceso a Programas).

**Artículo 66. Restricciones de acceso a información.** Para la generación de cuentas de usuario en los sistemas, así como para la asignación de perfiles, el director o jefe del área respectiva es el responsable de presentar la 'Solicitud de Usuarios y/o Perfiles de Acceso a los Sistemas de Cómputo.

El líder del área de tecnología será el encargado de generar los usuarios y sus respectivas contraseñas, para luego remitirlas a cada funcionario o usuario final, con la confidencialidad requerida. Para este proceso de debe otorgar a los usuarios acceso solamente a la información mínima necesaria para la realización de sus labores.

Esta tarea puede ser realizada utilizando una combinación de:

a) Seguridad lógica de la aplicación.
b) Ocultar opciones no autorizadas en los sistemas
c) Restringir el acceso a línea de comando
d) Limitar los permisos a los archivos de los sistemas (solo lectura)
e) Controles sobre la información de salida de los sistemas (reportes, consultas en línea, etc.)

**Artículo 67. Monitoreo del acceso y uso de los sistemas.**

a) **Sincronización del reloj.** Los relojes de todos los sistemas deben ser sincronizados para asegurar la consistencia de todos los registros de auditoría. El reloj debe estar sincronizado con la hora oficial colombiana.

b) **Responsabilidades generales**. El área de tecnología debe realizar monitoreo periódico de los sistemas como parte de su rutina diaria de trabajo. Este monitoreo no debe estar limitado solamente a la utilización del sistema, sino debe incluir el monitoreo del acceso de los usuarios a los sistemas.

c) **Registro de eventos del sistema**.

1. La actividad de los usuarios vinculada al acceso a información clasificada como CONFIDENCIAL o RESTRINGIDA. Debe ser registrada para su posterior inspección y verificación. El responsable de la información debe revisar dicho registro mensualmente.
2. Todos los eventos de seguridad relevantes de un computador que alberga información CONFIDENCIAL, deben ser registrados en un log de eventos de seguridad. Esto incluye errores en autenticación, modificaciones de datos, utilización de cuentas privilegiadas, cambios en la configuración de acceso a archivos, modificación a los programas o sistemas operativos instalados, cambios en los privilegios o permisos de los usuarios o el uso de cualquier función privilegiada del sistema.
3. Los logs (bitácoras) de seguridad deben ser almacenados por un periodo mínimo de 3 meses. El acceso a dichos logs debe ser permitido solo a personal autorizado. En la medida de lo posible, los logs deben ser almacenados en medios de "solo lectura".

## TITULO XIII
## REVISIÓN Y CUMPLIMIENTO

**Artículo 68. Cumplimiento normativo**. Toda ley, norma, estatuto, decreto, regulación o acuerdo contractual referente a los aplicativos y la información manejada en el IDEAR, debe ser documentada y revisada por el área jurídica del instituto. Los recursos informáticos de la entidad deben ser utilizados exclusivamente para tareas asociadas y vinculantes al negocio y servicios propios del IDEAR.

**Artículo 69. Registros de información.** Deben especificarse estándares de retención, almacenamiento, manejo y eliminación de registros de información, que son requeridos por normas legales u otras regulaciones. Dentro del cronograma de retención para estos registros, el cual se estipula realizar cada 3 meses, se debe incluir:

a) Tipo de información
b) Regulaciones o leyes aplicables a la información requerida
c) Fuentes de la información
d) Tiempos de retención requeridos
e) Requerimientos de traslado, intercambio, almacenamiento y distribución
f) Procedimientos de eliminación
g) Requerimientos de control específicos

**Artículo 70. Revisión de las Políticas de seguridad y cumplimiento técnico.** La Gerencia y los líderes de las respectivas áreas de la entidad, apoyados con el área de tecnología como administrador de la seguridad informática del IDEAR, deben asegurarse que las responsabilidades referentes a las políticas en seguridad de la información serán cumplidas y las funciones relacionadas a los cargos de cada uno de los funcionarios se ejecuten adecuadamente.

## TITULO XIV
## PROGRAMAS Y APLICATIVOS

**Artículo 71. Propiedad de los programas y aplicativos.** Cualquier programa, aplicativo o sistema codificado por algún funcionario o personal de la entidad y que esté dentro del alcance de su trabajo, así como aquellos adquiridos por el instituto son propiedad del IDEAR. Esto sujeto a las condiciones contractuales específicas para la adquisición de dichos sistemas, acordadas con los proveedores de los mismos o las condiciones de compra. Dentro de dichos contratos para el desarrollo de aplicativos externos, deben acordarse por escrito y deben señalar claramente el propietario de los derechos del programa. Si el IDEAR ejecuta el pago por el desarrollo del mismo, entra como propietario del producto final entregado (del licenciamiento, no del código fuente, el cual es propiedad intelectual del tercero).

**Artículo 72. Copia y/o distribución de software adquirido o licenciado.** Los contratos con proveedores y paquetes propietarios de software deben definir claramente los límites y alcance de su uso. Los funcionarios están desautorizados a copiar, reproducir, distribuir, utilizar y/o vender dicho software, de manera diferente a lo estipulado en el contrato. Toda infracción de los derechos de autor del software constituye un delito y está sujeto a las reglamentaciones correspondientes.

Los productos adquiridos o licenciados, que se ejecutan en cada uno de los equipos de cómputo del instituto no deben ser copiados o ejecutados en equipos diferentes a los establecidos, sin autorización expresa del proveedor y/o la Gerencia del instituto. Los funcionarios, personal del instituto o usuarios que realicen copias adicionales a las adquiridas o licenciadas, para uso o distribución propia, violarán los acuerdos legales y serán procesados como corresponde.

## TITULO XV
## ANEXOS

### Anexo A
### FORMATO REGISTRO DE FALLAS

**Nombre de la persona que reporta la falla:**

_____

**Email:** _____ **Cargo:** _____ **Tel:**

_____

**Fecha de la falla:** _____ **Hora de la falla:** _____

**Ubicación de la falla:** _____

**Descripción del error o problema:**

_____

_____

_____

**Descripción de la respuesta inicial ante el problema:**

_____

_____

**Descripción de la solución al problema:**

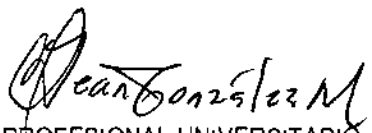
_____

_____

**Fecha de solución del problema:** _____ **Hora de solución del problema:** _____

**Responsable de solución del problema:** _____

**Firma Verificación y Aprobación del Registro**

| REVISÓ | APROBÓ |
|---|---|
|  PROFESIONAL UNIVERSITARIO PLANEACIÓN |  GERENTE |

| CONTROL DE CAMBIOS | | | |
|---|---|---|---|
| **FECHA** | **DESCRIPCIÓN DEL CAMBIO** | **VERSIÓN** | **MODIFICADO POR** |
| 15 de diciembre de 2017 | Adopción del Manual. Res. 441/2017 | 01 | |
| 12 febrero de 2019 | Acuerdo 02 - febrero 12 de 2019 | 02 | Prof. U. Requerimientos Tecnológicos |