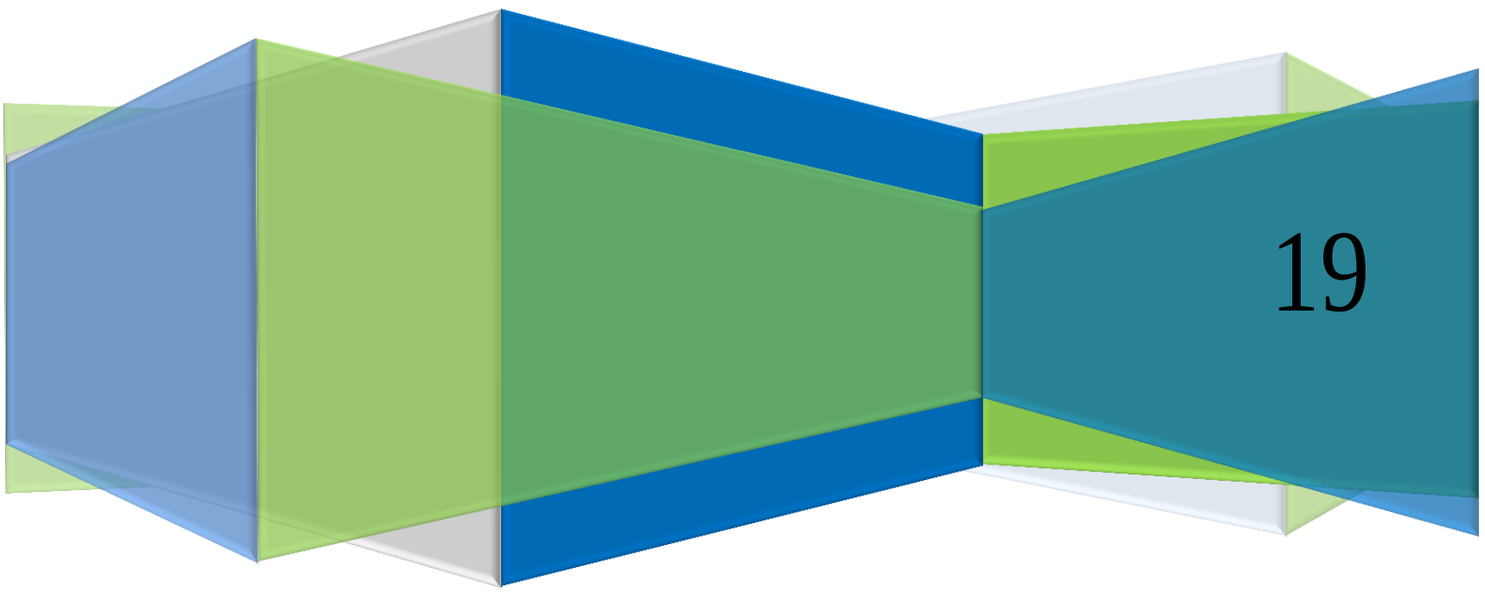
IDECESAR

INSTITUTO PARA EL DESARROLLO DEL CESAR - IDECESAR

PLAN DE SEGURIDAD DE LA INFORMACIÓN DOCUMENTAL Y SEGURIDAD DIGITAL



IDECESAR

EQUIPO DIRECTIVO

Luis Guillermo Castro Gonzales.
Gerente

Jose Victor Mestre
Asesor de Control Interno

Andrea Carolina Vilardy Rivero
Jefe de Gestión de Riesgos

Daniel Joaquín Pumarejo Buelvas
Jefe de Contabilidad y Presupuesto

María Carolina Lacouture Gutiérrez
Jefe Unidad de proyectos

Marta Niño Quiroga
Coordinadora de Crédito y Cartera

Tatiana Mendoza Maya
Asesora Jurídica

Ella Fidelina Fuentes Rodríguez
Tesorera

Lucas Francisco Monsalvo Hinojosa
Unidad de Emprendimiento

Yolima del Rosario Castilla Nieto
Apoyo Crédito y Cartera

Wilder Enrique Arias Ávila
Ingeniero de Sistemas

Enma Carolina Aroca Delgado
Secretaria

INTRODUCCIÓN

Hoy en día, la información está definida como uno de los activos más valiosos y primordiales para cualquier tipo de organización, la cual, sólo tiene sentido cuando está disponible y es utilizada de forma adecuada, integra, oportuna, responsable y segura, lo que implica, que es necesario que las organizaciones tengan una adecuada gestión de sus recursos y activos de información con el objetivo de asegurar y controlar el debido acceso, tratamiento y uso de la información.

El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razón por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial.

IDECESAR por medio de las oficinas de las TICs, Sistemas e Informática y la oficina de Riesgos elabora el siguiente documento Plan de Seguridad de la Información para que sea un instrumento que no solo concientice a los usuarios del Instituto sino para que también pongan en práctica las obligaciones (derechos y deberes) que en materia de seguridad de la información se estipulen en el presente documento.

Teniendo en cuenta la infraestructura y los servicios que presta Idecesar es necesario exigir a los usuarios que promuevan la superación de fallas y debilidades en lo relacionado con seguridad de la información para así cumplir con la responsabilidad misional del Instituto.

IDECESAR, debe cumplir con estándares de Seguridad en sus sistemas misionales, servicios y protección de la información, garantizando la confidencialidad de los datos, la disponibilidad del sistema de información y la red y la integridad de la información.

OBJETIVOS DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN DOCUMENTAL Y SEGURIDAD INFORMÁTICA

Presentar los elementos que conforman el plan de seguridad de la información y de la seguridad digital que deben conocer, acatar y cumplir todos los funcionarios de Idecesar, incluyendo contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el instituto.

Definir las directrices generales relacionadas con la seguridad de la información que junto con las demás políticas, normas y procedimientos que son aprobados como tales, constituyen el cuerpo normativo para la seguridad de información de IDECESAR.

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.

ALCANCE DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN DOCUMENTAL Y SEGURIDAD INFORMÁTICA.

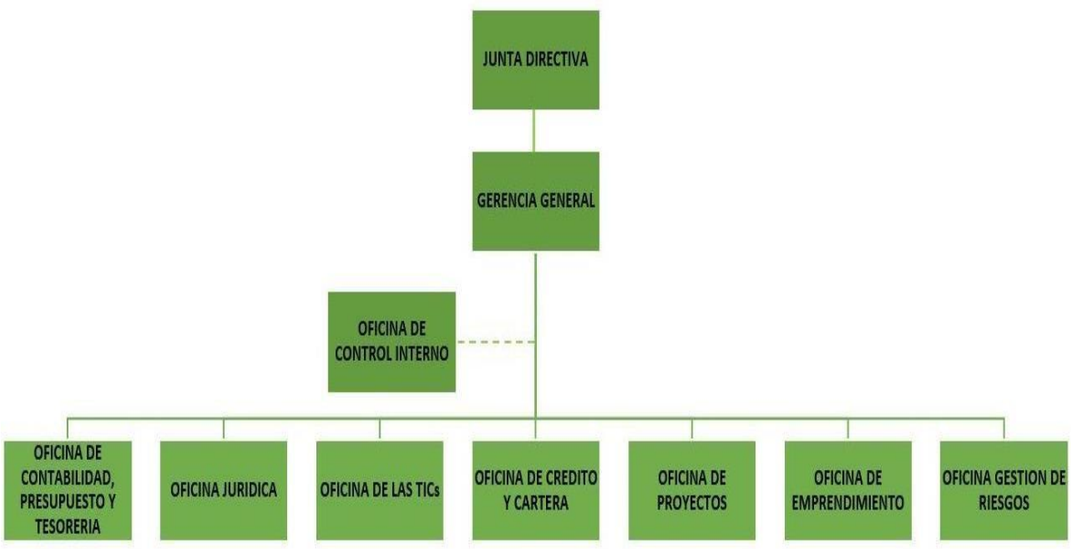
El ámbito de aplicación del plan de seguridad de la información documental y seguridad digital para el cual se desarrolla el presente documento son:

Los activos de información con que cuenta Idecesar, ya sea Datos, Aplicativos o Sistemas de Información, Personal, servicios informáticos, tecnologías y/o Infraestructura tecnológica, instalaciones y equipamiento auxiliar.

Procesos y subprocesos donde se gestione información de los sistemas misionales.

Estructura organizacional de Idecesar teniendo en cuenta los recursos tecnológicos y humanos, a los proveedores y prestadores de servicios, terceros que de alguna forma pudieran tener alguna manera habitual u ocasional de interacción con la información o con los equipos y dispositivos que almacenan tramitan o procesan.

Organigrama IDECESAR



TERMINOS Y DEFINICIONES

Activos de Información: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionada con el tratamiento de la misma que tenga un valor para la organización. Para el caso de Idecesar es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos del instituto. Estos activos se pueden clasificar de la siguiente manera:

- **Datos**: son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en Idecesar. *Ejemplo:* un archivo de Excel "directorio telefónico.xls", entre otro o más formato.
- **Aplicaciones**: es todo el software que se utiliza para la gestión de información. *Ejemplo:* SISTEMA CONTABLE INTEGRADO VISUAL TNS.
- **Personal**: es todo el personal de Idecesar (funcionarios), el personal subcontratado (Contratistas), los usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información del Instituto.
- **Servicios informáticos**: son los servicios de tecnologías informáticas prestadas por parte de la oficina de las TICs entre las cuales se distinguen:
    - **Servicios de cliente:** video conferencia, soporte a computadores personales.
    - **Servicio de seguridad informática:** manejo y administración de incidentes de seguridad, monitoreo y auditoría de seguridad.
    - **Servicios básicos**
    - **Servicios a servidores**
    - **Servicios de red:** internet, LAN, inalámbrica, telefonía.
    - **Servicios físicos:** cableado, UPS, Aires acondicionados, planta eléctrica.
- **Tecnologías**: también denominado infraestructura de tecnología informática y de las comunicaciones TICs. Son todos los equipos utilizados para gestionar la información y las comunicaciones. *Ejemplo*: equipos de cómputo, teléfonos, impresoras.
- **Instalaciones**: son todos los lugares donde se alojan los sistemas de información. *Ejemplo:* oficina de crédito y cartera.
- **Equipamiento auxiliar**: son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos. *Ejemplo:* aires acondicionados.

RESPONSABLES DEL CUMPLIMIENTO DEL PLAN

Todo el personal de IDECESAR y los terceros que interactúan de manera habitual u ocasional con los activos de información son responsables de informarse del contenido del cuerpo normativo de

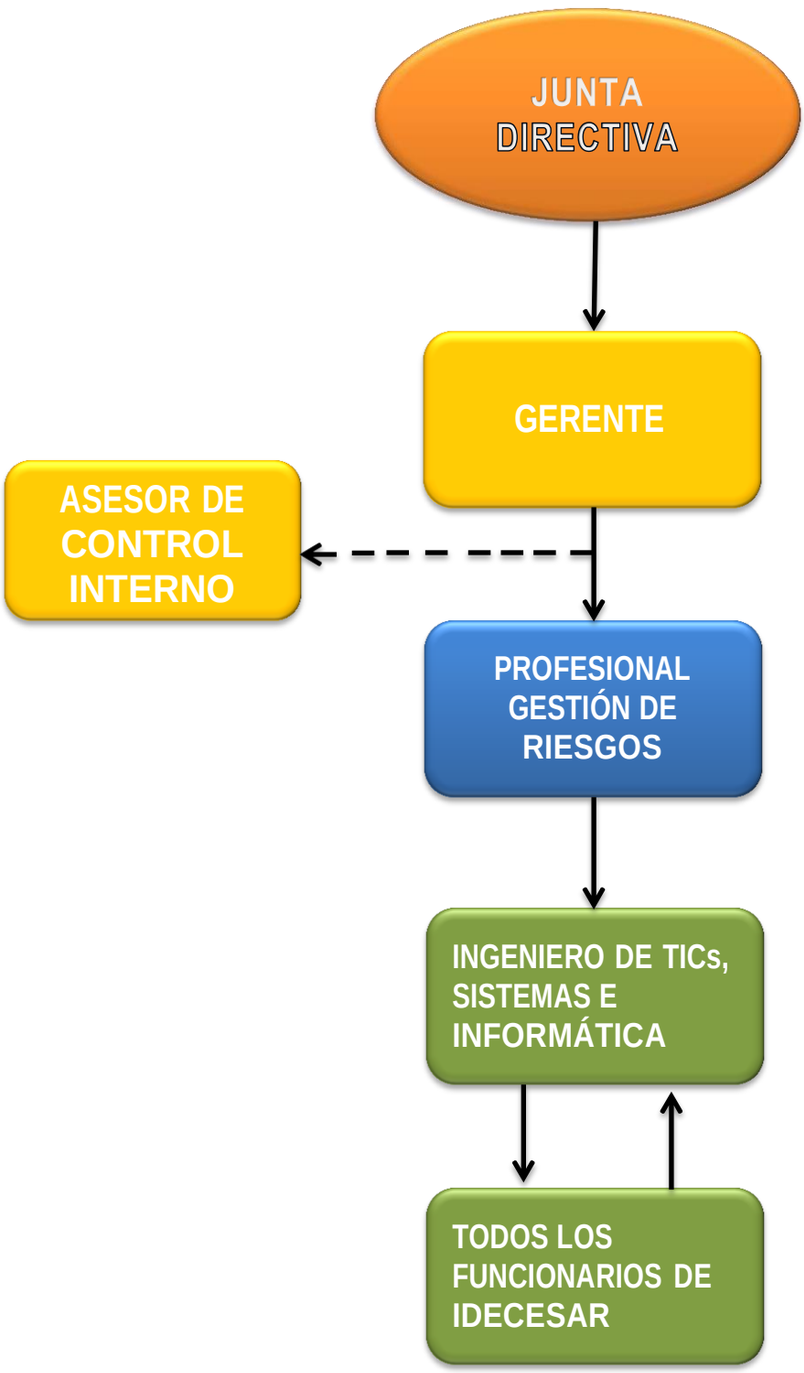
seguridad de información, cumplirlo y hacerlo cumplir en el desarrollo de sus tareas habituales, estas políticas de seguridad de información son de aplicabilidad a todo el personal del Instituto sin interesar su relación con la empresa, el área al cual se encuentre afectado o el nivel de tareas que desempeñe. El incumplimiento de las políticas de seguridad de información tendrá como resultado la aplicación de diversas sanciones conforme a la magnitud y características del aspecto no cumplido.

SEGURIDAD FÍSICA (RESTRICCIONES)

El acceso físico a cualquier activo de información tangible tales como servidores, elementos de red, documentos y otros elementos críticos de la infraestructura como transformadores y paneles eléctricos debe estar correctamente restringido.

ORGANIZACIÓN DE LA SEGURIDAD (ESTRUCTURA ORGANIZACIONAL)

En la administración de la seguridad de la información participan todos los funcionarios de IDECESAR. Dado el volumen de la información para IDECESAR es necesaria la existencia del área que administre la seguridad informática para garantizar un adecuado ejercicio de los procesos y funciones; IDECESAR, adopta una Estructura para el análisis, control y prevención de la seguridad informática, constituida de la siguiente forma:



RESPONSABILIDADES DEL INGENIERO DE LAS TICS EN IDECESAR

- Establecer y documentar las responsabilidades de la organización en cuanto a la seguridad informática.
- Mantener las políticas y estándares de seguridad en la información en IDECESAR.
- Identificar objetivos de seguridad, tales como prevención de virus, uso de herramientas de monitoreo etc.
- Definir metodologías y procesos relacionados con la seguridad informática.

- Comunicar aspectos básicos de seguridad de información a los funcionarios de IDECESAR. Esto incluye un programa de concientización para comunicar aspectos básicos y políticas.
- Desarrollar controles para la institución.
- Monitorear el cumplimiento de las políticas de seguridad de la información.
- Controlar e investigar incidentes de seguridad o violaciones de seguridad.
- Realizar una evaluación periódica de vulnerabilidades de los sistemas conformados por la red de datos de IDECESAR.
- Evaluar aspectos de seguridad de productos de tecnología, sistemas o aplicaciones utilizados en IDECESAR.
- Verificar que cada activo de información tecnológica de IDECESAR haya sido asignado a un propietario, el cual debe definir los requerimientos de seguridad tales como políticas de protección, perfiles de acceso, respuesta ante incidentes y sea el responsable final del mismo.
- Coordinación de todas las funciones relacionadas a seguridad, como seguridad física, seguridad de personal y seguridad de información almacenada en medios no electrónicos.
- Reportar periódicamente a la Gerencia.
- Administración de accesos a las principales aplicaciones de IDECESAR.
- Monitorear la aplicación de los controles de seguridad física de los principales activos de información.

RESPONSABILIDADES DE LOS USUARIOS

Las responsabilidades de los usuarios finales es decir, aquellas personas que utilizan la información de IDECESAR como parte de su trabajo diario están definidas a continuación:

- Mantener la confidencialidad de las contraseñas.
- Reportar supuestas violaciones de la seguridad de la información.
- Asegurarse de ingresar información adecuada a los sistemas.
- Adecuarse a las políticas de seguridad de IDECESAR.
- Utilizar la información de IDECESAR únicamente para los propósitos autorizados.

ACCESOS A TERCEROS

IDECESAR debe establecer para terceros al menos las mismas restricciones de acceso a la información que a un usuario interno, además el acceso a la información debe limitarse a lo mínimo indispensable para cumplir con el trabajo asignado, las excepciones deben ser analizadas y aprobados por el ingeniero de sistemas, esto incluye tanto accesos físicos como lógicos a los recursos de información del Instituto.

FUERZA DE SEGURIDAD

IDECESAR cuenta con servicios de vigilancia y seguridad privada de sus instalaciones para garantizar la adecuada protección de los intereses patrimoniales y realizar el control de entrada y salida de usuarios del personal de la entidad.
Todos los visitantes deben ser registrados en el acceso principal de las instalaciones. El guardia de seguridad será el responsable de la autorización del ingreso, el visitante recibirá una tarjeta de visitante identificada por colores que indicará la dependencia a la cual accederá en forma exclusiva.
Los visitantes, funcionarios y proveedores deben portar la tarjeta de identificación en lugar visible y en forma permanente dentro de las instalaciones de IDECESAR.

El ingreso a una persona a las áreas restringidas será solo con el debido acompañamiento en todo momento de la persona responsable del área.

Todos los empleados deben tener especial cuidado de no permitir el paso a personas no autorizadas a áreas restringidas.

Todo los computadores, equipos de comunicación, teléfonos propios, no deben moverse reubicarse o ser sacados de las instalaciones sin autorización del Ingeniero de las TICs, sistemas e informática.

EVALUACIÓN DE RIESGOS.

En IDECESAR el costo de las medidas y controles de seguridad no debe exceder la perdida que se espera evitar, por tal razón para la evaluación el riesgo se deben tener en cuenta:

- La matriz de Riesgo: Ver anexo #1
- Clasificación de acceso a la información

Seguidamente;

- Análisis de riesgos.
- Cumplimiento.
- Aceptación de riesgos.

CLASIFICACIÓN DE LA INFORMACIÓN

Para el proceso de clasificación de la información de IDECESAR se definirá de acuerdo al siguiente esquema:

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, con entidades externas.
Ejemplo: Planes Estratégicos, Datos de adquisiciones (antes de su anuncio), Negociaciones, Desarrollo de nuevos servicios, Juicios, Títulos valores.

Confidencial: Aquella en donde su divulgación no autorizada puede derivar en impactos importantes para la operación de la Dependencia, perdiendo principalmente la oportunidad.
Ejemplo: Información sobre operaciones y transacciones del Instituto, Resoluciones y Actas de Comités, información de clientes, presupuestos, nómina y compensaciones, reportes de auditoría, 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, Comunicados Internos, Manuales de funciones y de procedimientos.

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, etc.

La clasificación asignada a la información, solo puede ser cambiada por el propietario luego de justificar formalmente el cambio en dicha clasificación y debe ser examinada para determinar el impacto en IDECESAR si fuera divulgada o alterada por medios no autorizados.

Diagrama: *(Definir estándares de clasificación para adoptar una protección apropiada de activo).*

APLICACIÓN DE CONTROLES PARA LA INFORMACIÓN

Controles para la información digital

- La información en formato digital clasificada como general puede ser almacenada en cualquier sistema del instituto y se deben tomar las medidas necesarias para no mezclarla con otra clasificación.
- 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.
- Todo usuario que requiera acceso a la información clasificada como RESTRINGIDA O CONFIDENCIAL, debe ser autorizado por el propietario de la misma y por tanto deben ser documentadas.
- 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.
- Toda transmisión de información clasificada como Restringida, Confidencial, Privada, realizada hacia o a través de redes externas del Instituto debe realizarse utilizando un medio de transmisión seguro o utilizando técnicas de encriptación probadas.

- 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.
- 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.

Controles para la información no digital

- Todo documento que presente información clasificada como Restringida o Confidencial debe ser etiquetada en la parte superior e inferior de cada página según corresponda.
- Todo documento clasificada como Restringida o Confidencial debe presentar una caratula que muestre la clasificación a que corresponde.
- 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.
- Solo el personal formalmente autorizado debe tener acceso a información clasificada como Restringida o Confidencial.
- Los usuarios que utilizan documentos con información Restringida o Confidencial deben asegurarse de:

    - Almacenarlos en lugares adecuados.
    - Evitar que usuarios no autorizados accedan a dichos documentos.
    - Destruir los documentos si luego de su utilización dejan de ser necesarios.

ANÁLISIS DE RIESGOS

Los funcionarios responsables de la información y los encargados de su custodia son conjuntamente responsables del desarrollo de análisis de riesgo anual de los sistemas a su cargo, como parte del proceso de análisis se debe identificar las aplicaciones para la recuperación de la información ante desastres, se debe identificar:

- Áreas Vulnerables.
- Pérdidas potenciales.
- Seleccionar controles para mitigar los riesgos, el cual indiquen las razones para su respectiva inclusión o exclusión, (Seguridad de datos, planes de respaldo y recuperación y procedimientos de operación)

Se considera que el análisis de riesgo debe ser trasladado una vez exista cualquier cambio significativo en los sistemas, considerando la concordancia con el clima cambiante de las operaciones de IDECESAR.

ACEPTACIÓN DE RIESGOS

La gerencia del Instituto para el Desarrollo del Cesar puede obviar algún control o solicitud de protección y proceder a la aceptación del riesgo ya identificado, únicamente cuando ha sido demostrado que las opciones disponibles para lograr el cumplimiento han sido identificadas y evaluadas.

La aceptación del riesgo por falta de cumplimiento en controles y/o medidas de protección debe ser documentado y revisado por las áreas involucradas, seguidamente debe ser comunicado por escrito donde se notifique la aceptación del Riego por las áreas responsables de la administración de la Seguridad.

SEGURIDAD DEL PERSONAL.

Los estándares de seguridad relacionados al personal de IDECESAR deben ser aplicados para asegurarse que los 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. Deben desarrollarse estándares adicionales para asegurar que el personal sea consciente de todas sus responsabilidades y acciones apropiadas en el reporte de incidentes.

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

SEGURIDAD EN LA DEFINICIÓN DE PUESTOS DE TRABAJO RECURSOS.

El gerente de Idecesar y/o la oficina de Jurídica deberán notificar a todos los funcionarios de Idecesar ya sea empleados de plantas o contratistas la renuncia o despido de los empleados así como el inicio y el fin de los periodos de vacaciones de los mismos. Cualquier ítem entregado al empleado o contratista como computadores portátiles, llaves, tarjetas de identificación, software, datos, documentación, manuales, etc. deberán ser entregados a su supervisor encargado.

La seguridad de IDECESAR es responsabilidad de todos los empleados y de las personas involucradas con la entidad. Por ende, todos los empleados, contratistas, proveedores y personas

con acceso a las instalaciones e información de IDECESAR deben acatar los estándares documentados en la política de seguridad de IDECESAR e incluir la seguridad como una de sus responsabilidades principales.

Todos los dispositivos personales como computadores portátiles y dispositivos portátiles de memorias que interactúen con el sistema deberán ser reportados por el sistema de vigilancia a su entrada en la entidad.

CAPACITACIÓN DE USUARIOS.

El Ingeniero de sistemas es el funcionario de Idecesar encargado de promover constantemente la importancia de la seguridad digital a todos los usuarios de los sistemas de información de IDECESAR. El programa de concientización en seguridad debe contener continuas capacitaciones y charlas, adicionalmente se puede emplear diversos métodos como afiches y correos electrónicos, los cuales tienen como fin, recordarles permanentemente a los usuarios el papel importante que cumplen en el mantenimiento de la seguridad de la información.

PROCEDIMIENTOS DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD DIGITAL Y NO DIGITAL.

Si un empleado de IDECESAR detecta o sospecha la ocurrencia de un incidente de seguridad, tiene la obligación de reportarlo al Gerente de la entidad. Si se sospecha la presencia de un virus en un sistema, el usuario debe desconectar el equipo de la red de datos, notificar al personal encargado del área de sistemas, quien será el encargado de eliminar el virus antes de ser conectado nuevamente al equipo a la red de datos. Es responsabilidad del empleado (con la apropiada asistencia técnica) asegurarse que el virus haya sido eliminado completamente del sistema antes de reactivarse el sistema.

De igual forma, si el empleado en su actividad diaria detecta que el sistema de seguridad presenta algún tipo de vulnerabilidad debe reportarlo inmediatamente gerente y al mismo tiempo que al encargado del área de sistemas de la entidad, está prohibido al empleado de la entidad de IDECESAR realizar pruebas al igual que aprovechar dicha vulnerabilidad para beneficio propio o de terceros.

REGISTRO DE FALLAS EN EL SISTEMA

El personal encargado de operar los sistemas de información debe registrar todos los errores y fallas que ocurren en el procedimiento de información o en los sistemas de comunicaciones, estos registros deben incluir lo siguiente:

- Nombre de la persona que reporta la falla.
- Hora y fecha de la ocurrencia de la falla.
- Descripción del error o problemas.
- Responsable de solucionar el problema.
- Descripción de la respuesta inicial ante el problema.
- Descripción de la solución del problema.
- Hora y fecha en que se solucionó el problema.

Los registros de fallas deben ser revisados mensualmente. 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.

INTERCAMBIO DE INFORMACIÓN Y CORREOS ELECTRÓNICOS

Los mensajes de correo electrónico deben ser considerados en un memorándum formal, son considerados como parte de registro de IDECESAR y están sujetas a monitoreo y auditoria. Los sistemas de correo electrónico no deben ser usados para lo siguiente:

- Enviar cadenas de mensajes.
- Enviar mensajes relacionados a seguridad, exceptuando al personal encargado de esta en la entidad.
- Enviar propaganda de candidatos políticos.
- Actividades ilegales, no éticas e impropias.
- Actividades no relacionadas con las funciones de IDECESAR.

No deben utilizarse reglas de reenvió automático a direcciones que no pertenecen a la entidad de IDECESAR.

SEGURIDAD PARA DATOS EN TRÁNSITO

La información a ser transferida en medio digital o impreso debe ser etiquetada con la clasificación de información respectiva y detallada claramente el remitente y receptor. La información enviada por servicios postales debe ser protegida de accesos no autorizados mediante la utilización de:

- Paquete sellado
- Entrega en persona
- Firmado y sellado de un cargo

SEGURIDAD FÍSICA DE LAS INSTALACIONES DE PROCESAMIENTO DE DATOS

IDECESAR implementa medidas de seguridad física, con el fin de asegurar la integridad de las instalaciones, las medidas de protección son acorde con al nivel de clasificación de los activos y el valor de la información procesada y almacenada en el Instituto.

PROTECCIÓN DE LAS INSTALACIONES DE LOS CENTROS DE DATOS

Para IDECESAR el centro de procesamiento de datos o de cómputo se define como la estancia física contenedora de equipos de almacenamiento, procesos o transmisión de información, es decir abarca el conjunto de las instalaciones del Instituto, que incluye:

- Servidores, computadoras personales y periféricas.
- Equipos de telecomunicaciones.
- Centrales telefónicas, PBX.
- Armarios de alambrado o cables

Los controles son evaluados anualmente para compensar cualquier cambio con relación a los riesgos físicos, El gerente junto con el Ingeniero de Sistemas del Instituto deben conectarse para el diseño de los controles físicos de seguridad.

CONTROL DE ACCESO A LAS INSTALACIONES DE PROCESAMIENTO DE DATOS

El acceso a las instalaciones de procesamiento de datos está restringido únicamente al personal autorizado. IDECESAR, 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, IDECESAR establece el uso de llaves como mecanismos para impedir que puertas y tapas se puedan abrir. Las llaves están bajo la responsabilidad del Ingeniero de sistemas del Instituto, encargado de aumentar la protección de los bienes protegidos, así como del registro de la identificación del personal que ingrese a realizar algún tipo de actuación en los equipos, de la misma manera 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 procesamiento de datos debe ser aprobado por escrito por el ingeniero de sistemas del Instituto.

ADMINISTRACIÓN DE COMUNICACIONES Y OPERACIONES

Todos los procedimientos de operación de los sistemas son documentados y los cambios realizados a dichos procedimientos son autorizados por la gerencia.

Los procedimientos de encendido y apagado de los equipos también son documentados y los procedimientos para encender y apagar los computadores en IDECESAR son los siguientes:

ENCENDER EL COMPUTADOR

Para encender el computador se tiene en cuenta los siguientes pasos:

1. Los cables de poder deben conectarse a la toma de energía
2. Se prende el estabilizador, batería, pila o UPS (Sistema ininterrumpido de Potencia) si el computador lo posee.
3. Se enciende la CPU, presionando el botón encender (Power), en caso que se requiera.
4. Por último se enciende la pantalla como apoyo visual.

APAGADO DEL COMPUTADOR

Para apagar el computador se sigue los siguientes pasos:

1. Deben cerrarse todos los programas abiertos y guardar la información.
2. Se activa la ventana de menú de inicio presionando la tecla Windows.
3. Se pulsa flecha arriba una vez, para quedar en apagar y se pulsa la tecla Enter.
4. Se ubica con el cursor la opción apagar y se pulsa la tecla Enter. En esta lista de opciones también se encuentra: Cerrar sesión de administrador, Reiniciar, Suspender y en algunos computadores.
5. Se espera que la CPU deje de sonar, después de producir un sonido seco.
6. Se apaga la pantalla, si se estaba trabajando con ella, los parlantes si los tiene y por último, el estabilizador

PROTECCIÓN CONTRA VIRUS

El Ingeniero de Sistemas realizará esfuerzos para determinar el origen de la infección por virus informático, para evitar la reinfección de los equipos del instituto.

La posesión de virus o cualquier programa malicioso está prohibida a todos los usuarios. En caso tal, se tomarán medidas disciplinarias en donde se encuentren dichos programas en computadoras personales de usuarios.

Todos los archivos adjuntos recibidos a través del correo electrónico desde Internet son revisados por un antivirus antes de ejecutarlos, IDECESAR actualmente tiene a Bitdefender Total Security. Así mismo está restringido el uso de CDs, discos compactos y discos extraíbles provenientes de otra fuente que no sea la del mismo instituto, sin embargo para utilizar estos dispositivos deben pasar primero por el área de sistema para su respectiva revisión o que el funcionario lo analice por medio del antivirus de la institución.

El programa antivirus se encuentra habilitado en todas las computadoras de la entidad y debe ser actualizado periódicamente. En caso de detectar fallas en el funcionamiento de dichos programas éstas deben ser comunicadas al área de soporte técnico.

El programa antivirus está configurado para realizar revisiones automáticas al conectar cualquier dispositivo externo llámese cd, USB, etc., así como también realiza revisiones periódicas para la detección de virus en los medios de almacenamiento de las computadoras de IDECESAR.
Se cuenta con un procedimiento para el monitoreo de los virus detectados.

Es obligación del personal del instituto, emplear sólo los programas cuyas licencias han sido obtenidas por el mismo y forman parte de su plataforma estándar.

Todo el personal del institutito deberá utilizar los protectores de pantalla y/o papel tapiz autorizados por la Institución.

COPIAS DE RESPALDO

Los usuarios de Idecesar deben generar copias de respaldo de información crítica transfiriendo o duplicando archivos a las carpetas personales establecida en la nube para dicho fin, previo compromiso adquiridos para con el Instituto y supervisado por el ingeniero de Sistemas.

El Ingeniero de Sistema es el funcionario encargado de salvaguardar la información que se generen copias de respaldo del software utilizado por Idecesar que se encuentra en el servidor del instituto.

Los mensajes electrónicos, así como cualquier información considerada importante, son guardados en copias de respaldo y retenidos por dispositivos automáticos

SEGURIDAD EN EL USO DEL CORREO ELECTRONICO

El uso inapropiado de los correos electrónicos en los equipos de Idecesar expone al instituto a riesgos innecesarios como ataque de virus, compromiso de las redes y sistemas. A continuación se ofrece una guía y unos requerimientos mínimos que se deben tener para el uso adecuado del correo electrónico:

- Utilización de la cuenta de correo con fines pertinentes a los procesos de Idecesar.
- Respetar las cuentas de otros usuarios.
- No mandar ni contestar cadenas de correo o cualquier otro esquema de "pirámide" de mensajes.
- No usar su cuenta para fines comerciales.
- No se debe transmitir virus o programas de uso mal intencionado.
- Los usuarios no deben leer correo ajeno ni generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.
- No introducir software malicioso en la red o en los servidores (virus, worms, ráfagas de correo electrónico no solicitado, etcétera).
- No revelar la clave o código de su cuenta, o permitir su uso a terceros para actividades ajenas a la misión de Idecesar.
- Se prohíbe el uso del sistema con el fin de realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil.
- No hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios de Idecesar.

CONTROL DE ACCESO A DATOS

Los datos o la información que se manejan en las diferentes aplicaciones o sistemas de información en Idecesar deben estar adecuadamente protegidos contra modificaciones no autorizadas, divulgación o destrucción. Por tal motivo se configuran unos controles de acceso que previenen y evitan dichos riesgos.

IDENTIFICACIÓN DEL USUARIOS

- En Idecesar Cada usuario de un sistema, debe ser identificado de manera única y el acceso del usuario así como su actividad en los sistemas debe ser controlado, monitoreado y revisado.
- Los 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.
- 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.

- Todos los sistemas deben proveer pistas de auditoría del ingreso a los sistemas y violaciones de los mismos.

VIGENCIA EN LAS CONTRASEÑAS

Todas las contraseñas deben expirar dentro de un periodo que no exceda los noventa (90) días.

REUTILIZACIÓN DE LAS CONTRASEÑAS

No debe permitirse la reutilización de ninguna de las 5 últimas contraseñas. Esto asegura que los Usuarios no utilicen las mismas contraseñas en intervalos regulares.
Los usuarios no deben poder cambiar sus contraseñas más de una vez al día.

INTENTOS FALLIDOS DE INGRESOS

Todos los sistemas deben estar configurados para deshabilitar los identificadores de los usuarios en caso de ocurrir (3) intentos fallidos de autenticación.

SEGURIDAD DE CONTRASEÑA

Es importante que todos los empleados protejan sus contraseñas, debiéndose seguir las siguientes regulaciones:

- Bajo ninguna circunstancia, se debe escribir las contraseñas en papel, o almacenarlas en medios digitales no encriptados.
- Las contraseñas no deben ser divulgadas a ningún otro usuario salvo bajo el pedido del gerente, con autorización del Ingeniero de sistemas del Instituto. Si se divulga la contraseña, esta debe ser cambiada durante el próximo ingreso.
- 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.
- Los sistemas no deben mostrar la contraseña en pantalla o en impresiones, para prevenir que éstas sean observadas o recuperadas.
- El control de acceso a archivos, bases de datos, computadoras y otros sistemas de recursos mediante contraseñas compartidas está prohibido.

CONTROLES DE ACCESO A PROGRAMAS

Los controles de acceso de programas deben asegurar que los usuarios no puedan acceder a l la información sin autorización.

-Los programas deben generar una pista de auditoría de todos los accesos y violaciones.

-Las violaciones de los controles de acceso deben ser registradas y revisadas por el propietario o por el ingeniero de sistemas del Instituto quien es el custodio de los datos.

-Las violaciones de seguridad deben ser reportadas al gerente y al área responsable de la administración de la seguridad de la información que para el caso recae en el ingeniero de sistemas del Instituto.

-Se debe tener cuidado particular en todos los ambientes para asegurar que ninguna persona tenga control absoluto. Los operadores de sistemas, por ejemplo, no deben tener acceso ilimitado a los identificadores de superusuario. Dichos identificadores de usuario, son solo necesarios durante una emergencia y deben ser cuidadosamente controlados por la gerencia, quien debe realizar un monitoreo periódico de su utilización.

RESPONSABILIDADES DEL USUARIO FRENTE AL USO DE LOS EQUIPOS DE CÓMPUTO

- Todo equipo de cómputo, alquilado o de propiedad de IDECESAR, serán usados solo para actividades relacionadas a la actividad del Instituto.
- Los equipos de IDECESAR no pueden ser usados para desarrollar software para negocios personales o externos al él.
- Los equipos no deben ser usados para preparar documentos para uso externo, salvo bajo la aprobación escrita del gerente.
- Se debe implementar protectores de pantallas en todas las computadoras personales y servidores, activándose luego de cinco (5) minutos de inactividad.

LINEAMIENTOS PARA EL USO DE LOS COMPUTADORES EN IDECESAR

La instalación de software en los computadores de IDECESAR, es una función exclusiva del Área de las TIC, Sistemas e Informática.

Los usuarios que hagan uso de equipos institucionales en préstamo, NO deberán almacenar información en estos dispositivos y deberán borrar aquellos que copien en estos al terminar su uso.
Los usuarios no deben mantener almacenados en los discos duros de los computadores de Idecesar archivos de vídeo, música, fotos y cualquier tipo de archivo que no sean de carácter institucional.

En el Disco C:\ de los computadores de Idecesar se tiene configurado el sistema operativo, aplicaciones y perfil de usuario, la persona que haga uso de los equipos deberá abstenerse de realizar modificaciones a éstos archivos.

El préstamo de equipos de cómputo, computadores portátiles y vídeo bean, se debe tramitar a través de la asistente de gerencia y/o el área de las TIC, Sistemas e Informática con previa solicitud escrita. Los equipos que ingresan temporalmente a IDECESAR que son de propiedad de terceros: deben ser registrados en los controles de acceso del instituto y su retiro; posteriormente IDECESAR no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones.

El Área de las TIC, Sistemas e Informática no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de IDECESAR.

Los equipos de uso personal, que no son de propiedad de IDECESAR, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por el Área de las TIC, Sistemas e Informática de IDECESAR.

SEGURIDAD DE LOS COMPUTADORES

Se debe mantener un inventario actualizado de todo el software y hardware existente en IDECESAR.

- Todo traslado o asignación de equipos debe ser requerida al gerente o al ingeniero de sistemas del Instituto y es responsabilidad del ingeniero de sistemas, la verificación y realización del requerimiento.
- Es de responsabilidad del usuario, efectuar un correcto uso del equipo de cómputo que le fue asignado, así como de los programas en él instalados; cualquier cambio y/o traslado deberá ser solicitado con anticipación al ingeniero de sistemas del instituto. Asimismo, el usuario debe verificar que cualquier cambio y/o traslado del Equipo de Cómputo que le fue asignado, se realice por medio del ingeniero de sistemas del instituto, así como también la instalación o retiro de software.

Cualquier computador o portátil perteneciente al IDECESAR debe ser únicamente utilizada para propósitos de negocios y servicios de la entidad. Estas computadoras pueden ser utilizadas de las siguientes maneras:

- Como un terminal comunicándose con otra computadora.
- Como una computadora aislada que realice su propio procesamiento sin comunicación con ninguna otra computadora.

Sin importar su uso, las medidas de seguridad deben ser implementadas en todas las computadoras personales:

- Una vez habilitada la computadora, ésta no debe dejarse desatendida, incluso por un periodo corto.
- Todos las, cintas, CD discos 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.
- 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
- Todos los programas instalados en las computadoras deben ser legales, aprobados y periódicamente inventariados.
- Solo los programas adquiridos o aprobados por IDECESAR, serán instalados en las computadoras del Instituto.
- El uso de programas de juegos, de distribución gratuita (freeware o shareware) o de propiedad personal está restringida, salvo que éste sea aprobado por la gerencia y se haya revisado la ausencia de virus en el mismo.

LINEAMIENTOS PARA EL USO DE INTERNET

La infraestructura, servicios y tecnologías usados para acceder a internet son propiedad de IDECESAR, por lo tanto se reserva el derecho de monitorear el tráfico de internet y el acceso a la información, respetando en todo momento el derecho a la privacidad y a la seguridad de los datos personales consagrados en la Ley 1581 de 2012.

No se permite la navegación a sitios web con contenidos contrarios a la ley o a las políticas de IDECESAR o que representen peligro para la entidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por el IDECESAR. El acceso a este tipo de contenidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del gerente de IDECESAR.

La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio.

La navegación en Internet debe realizarse de acuerdo con las labores asignadas al funcionario, contratista o colaborador y en todo momento buscando el cumplimiento de las funciones misionales de Idecesar.

No está autorizado el uso de Internet para descargar material sujeto a derechos de autor, sin el cumplimiento de los requisitos legales que están establecidos.

LINEAMIENTOS PARA SERVICIO DE ALMACENAMIENTO EN REDES PÚBLICAS (NUBE - INTERNET)

Descarga de Archivos

IDECESAR permite a los usuarios, la descarga de archivos desde los sistemas de almacenamiento ubicados en las redes públicas (Internet), únicamente con fines institucionales, la cual será supervisada con las herramientas de seguridad de la Información, destinadas para ese fin.

Carga de Archivos

El acceso a servicios de almacenamiento de información en plataformas públicas, personales o privadas como Dropbox, Google Drive, OneDrive, etc., con la finalidad de realizar almacenamiento de información del Instituto el cual debe ser aprobado por el Área de las TIC, Sistemas e Informática.

LINEAMIENTOS PARA USO DE PUNTOS DE RED DE DATOS (RED DE ÁREA LOCAL – LAN)

Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos Institucionales.

La instalación, activación y gestión de los puntos de red es responsabilidad del Área de las TIC, Sistemas e Informática.

LINEAMIENTOS DE USO DE IMPRESORAS Y DEL SERVICIO DE IMPRESIÓN

Los documentos que se impriman en las impresoras de IDECESAR deben ser de carácter institucional.

Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiadora) para que no se afecte su correcto funcionamiento.

Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar al Área de las TIC, Sistemas e Informática.

Los funcionarios en el momento de realizar impresiones de documentos con clasificación restringida, confidencial o privada, debe mantener control de la impresora, por lo cual no la deberán dejar desatendida, preservando la confidencialidad de la información.

POLÍTICAS DE SEGURIDAD DEL CENTRO DE DATOS Y CENTROS DE CABLEADO

Estas políticas consisten en asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

En las instalaciones del centro de datos o de los centros de cableado, No está permitido:

• Fumar dentro del centro de datos o de los centros de cableado.

• Introducir alimentos o bebidas al centro de datos o de los centros de cableado

• El porte de armas de fuego, corto punzantes o similares.

• Mover, desconectar y/o conectar equipos de cómputo o cables sin autorización.

• Modificar la configuración del equipo o intentarlo sin autorización.

• Alterar software instalado en los equipos sin autorización.

• Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.

• Extraer información de los equipos en dispositivos externos.

• Abuso y/o mal uso de los sistemas de información.

• Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

LINEAMIENTO DE SEGURIDAD Y CONTROL DE ACCESO AL CENTRO DE DATOS Y CENTROS DE CABLEADO

No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado por el Jefe del Área de las TIC, Sistemas e Informática.

Se debe llevar un control de ingreso y salida del personal que visita el centro de datos, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.

CUMPLIMIENTO DEL MANUAL

Las disposiciones contenidas en este Plan, son de obligatorio cumplimiento por parte de todos los destinatarios, su inobservancia se sancionará conforme a las normas administrativas pertinentes.

OSWALDO MAURICIO ANGULO AGUDELO

Gerente

ORIGINAL FIRMADO

Proyectó:
Wilder Arias.
Andrea V.

IDECESAR

ANEXO

IDECESAR

MATRIZ DE RIESGO TECNOLOGICO IDECESAR

	Categorias de Activos	Código	Descripción
Activos de Información IDECESAR	Datos	D1	Archivo digital con información contable del Instituto
		D2	Archivos físicos de respaldo de la contabilidad
		D3	Archivo digital con información Institucional
		D4	Archivos fisicos con información Institucional
		D5	Archivos físicos de clientes del Instituto
		D6	Archivos digitales con información de los clientes del Instituto
		D7	Archivos digitales con información de los correos corporativos
	Servicios	S1	Página web con información de servicios institucionales
		S2	Correo corporativo
		S3	Software suministrado por compañía asociada para el manejo de su información
		S4	Conexión a labase de datos Institucional
		S5	Redes sociales
		S6	Conexión a base de datos de entidades externas
	Hardware	H1	Router
		H2	Servidor
		H3	Computadores
		H4	Impresoras/Scanner
		H5	Impresora de red
		H6	Fax
		H7	Sistema de clabeado para la red interna
	Software	SO2	Sistema operativo de los equipos de computo (Windows 7, Windows 8, Windows 10, Windows server 2012.)
		SO3	Office 2010
		SO4	Software antivirus
		SO5	Navegadores de internet (internet explorer, Google Chrome)
		SO6	Sistema Contable integral y credito y cartera (servidor de archivo)
		SO7	Acrobat Reader
	Redes de comunicación	RC1	Celulares corporativos
		RC2	Conexión a internet
		RC3	Telefono fijo
		RC4	VPN
	Personas/Recursos Humanos	P1	Gerente
		P2	Asesor de control interno
		P3	Gestión de riesgos
		P4	Contabilidad y presupuesto
		P5	Proyectos
		P6	Emprendimiento
		P7	Credito y cartera
		P8	Asesor jurídico
		P9	Tesorería
		P10	Ingeniero de las Tics, sistemas e informática
		P11	Secretaria
	Soporte de Información	SI1	Usb
		SI2	Cd
		SI3	Discos duro
		SI4	Nube
		SI5	Acetas para información contable
		SI6	Acetas para información de pólizas
		SI7	Acetas con información Institucional
	Soporte Auxiliar	SA1	Cajas de seguridad de Archivo
		SA2	Acetas
		SA3	Carpetas
	Instalaciones	I1	Calle 28 # 6A- 15 Barrio Santa Rosa