PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION- PETI

AÑO 2023

Bucaramanga, 2023

Así mismo, este PETI se estructurará con fundamento en el artículo 74 de la Ley 1474 de 2011, en el artículo 147 de la Ley 1955 de 2019, en la Guía Técnica "G.ES.06 Guía Cómo

Elaborar el Plan Estratégico de Tecnologías de la Información – PETI", Versión 2.0 del 10 de julio de 2019 del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

1. OBJETIVOS

1.1 Objetivo General

Formular la estrategia de las Tecnologías de Información (TI) mediante la cual el IDESAN busca alinear las TI que soportan sus procesos institucionales, con su misión, su visión y sus objetivos estratégicos para convertirlas en agentes clave en la transformación digital del IDESAN en el marco de la Política de Gobierno Digital de Colombia, a través de su gestión, aprovechamiento y uso óptimos y eficientes que agreguen valor a los servicios institucionales.

1.2 Objetivos Específicos

- Presentar el análisis de la situación actual de la Entidad para cada uno de los dominios de tecnología establecidos en el marco de referencia de la arquitectura empresarial establecidos por MINTIC y para cada uno de los propósitos establecidos en la política de Gobierno Digital; a partir de la ejecución de un ejercicio ágil sobre los habilitadores de arquitectura, seguridad y servicios ciudadanos digitales.

- Definir la visión estratégica de la Entidad en cuanto a las tecnologías de la información y las comunicaciones a partir del análisis de la situación actual; de los diferentes motivadores y directores del negocio; de las prospectivas tecnológicas; y, de las metas y objetivos definidos en los diferentes planes estratégicos de nivel nacional y departamental.

- Construir el mapa de ruta, materializado en propuestas de proyectos, cuya ejecución conlleve a la Entidad a obtener la visión estratégica que en cuanto a las tecnologías de la información y las comunicaciones se ha propuesto.

INTRODUCCIÓN

El Plan Estratégico de Tecnologías de la Información – PETI del Instituto Financiero para el Desarrollo de Santander, estará alineado con la misión, visión y objetivos estratégicos de la entidad, estableciendo la hoja de ruta de implementación de los proyectos de TI y la continuidad de los proyectos y servicios de TI existentes para la vigencia.

De igual manera estará articulado al modelo integrado de planeación y gestión (MIPG) y en los habilitadores de arquitectura, servicios ciudadanos digitales y seguridad y privacidad de la información, establecidos en la Política de Gobierno Digital de Ministerio de Tics, redundando en beneficios a los grupos de valor de la entidad (servidores públicos, entidades y ciudadanos).

Este documento incorporara las necesidades de las áreas que conforman la entidad, el marco normativo, situación actual, entendimiento estratégico, continuidad del negocio, procesos institucionales, activos de información, sistemas de información, infraestructura de TI y el análisis de mejores prácticas en la industria de TI, para la planificación y ejecución de los proyectos de las tecnologías de información y comunicaciones.

El Plan Estratégico de Tecnologías de la Información (PETI) del INSTITUTO FINANCIERO PARA EL DESARROLLO DE SANTANDER (IDESAN), estará formulado para el periodo 2021-2022 de conformidad con lo ordenado por la Ley 1951 de 2019, el artículo 215 de la Ley 1955 de 2019 refleja la realización de un ejercicio de planeación estratégica de las adquisiciones, desarrollo, soporte, mantenimiento y uso y apropiación de las tecnologías de la información y las comunicaciones.

El objeto fundamental del PETI es constituirse en el marco conceptual que oriente al IDESAN en la toma de decisiones respecto a las tecnologías y sistemas de información y comunicaciones y apoye de manera eficiente el cumplimiento de los objetivos institucionales, para lo cual se alinea con el Objetivo Estratégico institucional ***6 FORTALECER TECNICA ADMINISTRATIVA Y FINANCIERAMENTE AL INSTITUTO, PARA AFRONTAR LOS RETOS COMO EL INFI AL SERVICIO DE NUESTRO DEPARTAMENTO***. Mediante las siguientes cuatro Iniciativas Estratégicas:

1. Estrategia TI y Gobierno TI
2. Infraestructura Digital
3. Gestión de Seguridad y Privacidad de la Información
4. Sistemas de Información, Datos y Servicios Digitales

2. MARCO LEGAL

- Decreto 620 de 2020, "Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 Y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales".

- Decreto 2106 de 2019, Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Publica Efectiva.

- Decreto 612 de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- Decreto 1008 de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

- Ley 1581 de 2017, La cual se dictan disposiciones generales para la Protección de Datos Personales.

- Decreto 1499 de 2017, Por medio del cual se modifica el Decreto 1083, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753.

- Decreto 415 de 2016, Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones.

- Decreto 2433 de 2015, Por el cual se reglamenta el registro de TIC y se subroga el título 1 de la parte 2 del libro 2 del Decreto 1078, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Ley 1712 de 2014, Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

- Decreto 2573 de 2014, Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

- Decreto 2693 de 2012, Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones.

- Ley 527 de 1999, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

3. DEFINICIONES Y ABREVIATURAS

3.1 DEFINICIONES

Arquitectura Empresarial: Es una práctica estratégica que consiste en analizar íntegramente las entidades desde diferentes perspectivas o dimensiones, con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria. El objetivo es generar valor a través de las Tecnologías de la Información para que se ayude a materializar la visión de la entidad.

Componentes de información: Término utilizado para referirse bajo un único nombre al conjunto de los datos, la información, los servicios de información y los flujos de información.

Dominios: Son los componentes que conforman la estructura del Marco de Referencia de Arquitectura. Los dominios son las dimensiones desde las cuales se debe abordar los ejercicios de Arquitectura. Los dominios agrupan y organizan los lineamientos.

Estrategia TI: Conjunto de principios, objetivos y acciones concretas que reflejan la forma en la cual una entidad decide utilizar las Tecnologías de la Información para permitir el logro de su misión de una manera eficaz. La Estrategia TI es una parte integral de la estrategia de una entidad, la cual se debe reflejar en el PETI.

Gestión TI: Es una práctica que permite operar, innovar, administrar, desarrollar y usar apropiadamente las tecnologías de la información (TI), con el propósito de agregar valor para la organización. La gestión de TI permite a una organización optimizar los recursos, mejorar los procesos de negocio y de comunicación y aplicar las mejores prácticas.

Gobierno de TI: Es una práctica, orientada a establecer unas estructuras de relación que alinean los procesos de negocio con los procesos, recursos y estrategias de TI, para agregar valor a las organizaciones y apoyar el cumplimiento de sus objetivos estratégicos. El gobierno de TI gestiona y controla los riesgos, mide el desempeño de TI, busca optimizar las inversiones de TI y establecer un esquema de toma de decisiones de TI. El gobierno de TI es parte del gobierno corporativo o empresarial.

Infraestructura Digital: Es una estructura conceptual y tecnológica basada en hardware y software, mediante la cual se soportan los servicios de TI requeridos para el funcionamiento de la entidad y que esta brinda a la ciudadanía en general. En este tipo de servicios los Acuerdos de Nivel de Servicio son críticos para garantizar algunos atributos de calidad como disponibilidad, seguridad, confiabilidad, etc.

Interoperabilidad: Es "la capacidad de las organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio para interactuar hacia objetivos mutuamente beneficiosos, con el propósito de facilitar la entrega de servicios digitales a ciudadanos, empresas y a otras entidades, mediante el intercambio de datos entre sus sistemas TIC". Esta es la definición de Interoperabilidad acogida para el Gobierno Digital.

Lineamiento: Es una orientación de carácter general, corresponde a una disposición o directriz que debe ser implementada en las entidades del Estado colombiano.

Marco de interoperabilidad: Es la estructura de trabajo común donde se alinean los conceptos y criterios que guían el intercambio de información. Define el conjunto de principios, recomendaciones y directrices que orientan los esfuerzos políticos, legales, organizacionales, semánticos y técnicos de las entidades, con el fin de facilitar el intercambio seguro y eficiente de información.

PETI: El Plan Estratégico de Tecnologías de la Información (PETI) es un documento que define la estrategia bajo la cual se espera que las TI se integren con la misión, visión y objetivos organizacionales.

Plan de comunicación de la Estrategia de TI: Toda estrategia debe ser comunicada de manera adecuada a los distintos interesados, dentro y fuera de una institución. El plan de comunicación define los tipos de usuarios a los que se informará, los tipos de contenido y medios de comunicación por usar, para divulgar la Estrategia de TI. Este plan es uno de los componentes de un PETI.

Proyecto: Es un conjunto estructurado de actividades relacionadas para cumplir con un objetivo definido, con unos recursos asignados, con un plazo definido y un presupuesto acordado.

Servicios Ciudadanos Digitales: Es el conjunto de soluciones y procesos transversales que brindan al Estado capacidades y eficiencias para su Transformación Digital, para lograr una adecuada interacción del ciudadano con el Estado, garantizando el derecho a la utilización de medios electrónicos ante la administración pública.
Servicio de información: Consiste en la entrega de información de valor para los usuarios de una entidad a través de un proveedor de servicio interno o externo. Un servicio de información se describe a través de un contrato funcional (qué recibe como entrada y qué produce como salida) y un conjunto de acuerdos de servicio que debe cumplir.

Trabajo Colaborativo: Es la capacidad basada en el uso de tecnologías de la información y comunicación (TIC), que permite la interacción dinámica, independiente y en tiempo real de los colaboradores para aportar a un propósito común o proyecto compartido.

Valor público: Este es el fin último del uso de la tecnología en la relación del Estado, ciudadanos, usuarios y grupos de interés. El valor público se relaciona con el desarrollo social, la gobernanza, la garantía de derechos, la satisfacción de necesidades, la prestación de servicios de calidad y el mejoramiento de las condiciones de vida de la sociedad. No sólo es hacer uso de las tecnologías, sino cómo las tecnologías ayudan a resolver problemas reales. Valor público también es lograr que el Estado llegue a donde no llega el mercado, satisfaciendo necesidades y problemáticas.

3.2 ABREVIATURAS

- CTeI: Ciencia, Tecnología e Innovación
- Min Ciencias: Ministerio de Ciencia, Tecnología e Innovación
- OTSI: Oficina de tecnologías y Sistemas de Información
- PEI: Plan Estratégico Institucional
- SIGP: Sistema de Información de Gestión de Proyectos
- SIVEAP: Sistema de Información de Verificación, Evaluación y Ajuste Provisional. TI: Tecnologías de la Información
- TIC: Tecnologías de la Información y Comunicaciones

4. POLITICAS TI

4.1 Políticas Generales de TI, en las cuales se encuentran lineamientos asociados a la divulgación, periodicidad de actualización de la política de TI, la necesidad de incluir esta temática en las actividades de inducción institucional, además los sujetos obligados del cumplir estos lineamientos entre otras directrices de carácter general.

4.2 Políticas de adquisiciones, renovaciones y suscripciones tecnológicas, las cuales comprenden lineamientos relacionados con las adquisiciones de TI y su alineación con el manual de contratación y procedimiento de gestión contractual de la Entidad. También, siguiendo los lineamientos de Arquitectura Empresarial, incluye el lineamiento sobre la realización de procesos de adquisición de TI utilizando Acuerdos Marco de Precios, o Servicios de Agregación por demando: así como lineamientos sobre la transferencia de conocimiento de los bienes y servicios de TI adquiridos.

4.3 Políticas de Sistemas de Información, en ésta se dan directrices asociadas a la creación o desarrollo o compra de nuevos aplicativos o sistemas de información, así como al mantenimiento y soporte de los sistemas de información existentes y de propiedad del IDESAN.

Gobierno Digital es la política de MIPG que busca promover el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones -TIC, para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor públicoen un entorno de confianza digital.

La política de Gobierno Digital contribuye a la Transformación Digital del sector público, la cual implica un cambio en los procesos, la cultura y el uso te de la tecnología (principalmente tecnologías emergentes y de la Cuarta Revolución Industrial), para el mejoramiento de las relaciones externas de las entidades de Gobierno, a través de la prestación de servicios más eficientes.

Esto significa, que a través del Gobierno Digital se busca que tanto el Estado como ciudadanos y diferentes actores de la sociedad, hagan uso de las TIC como herramientas que permiten optimizar la gestión de las entidades, interactuar de manera ágil y coordinada, trabajar conjuntamente en el diseño y desarrollo de políticas, normas, proyectos y servicios, y dar solución a problemáticas y necesidades de interés público.

En este sentido, la política de Gobierno Digital actúa como una política transversal que se relaciona con las demás políticas del Modelo Integrado de Planeación y Gestión, facilitando su implementación y potenciando los beneficios tanto para las entidades del Estado, como para ciudadanos, usuarios y grupos de interés. A partir de ello, políticas como Talento Humano, Planeación Institucional, Gestión Presupuestal, Transparencia y Acceso a la Información Pública, Fortalecimiento Organizacional y Simplificación de Procesos, Servicio al Ciudadano, Participación ciudadana, Racionalización de Trámites, Gestión Documental, Seguridad Digital, Gestión del conocimiento y la innovación, entre otras, son apalancadas a través de Gobierno digital.

Específicamente, la política de Gobierno Digital cuenta con cinco grandes propósitos que se pretenden alcanzar a través del uso y aprovechamiento de las TIC, por parte del Estado y de los actores de la Sociedad que se relacionan con éste:

- Habilitar y mejorar la provisión de servicios digitales de confianza y calidad.
- Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.
- Tomar decisiones basadas en datos, a partir del aumento del uso y aprovechamiento de la información.
- Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto.
- Impulsar el desarrollo de territorios y ciudades inteligentes, para la solución de retos y problemáticas sociales a través del aprovechamiento de las TIC.

Marco Normativo

- Ley 1955 de 2019 art. 147 y 148
- Decreto 2106 de 2019 art. 8 -17
- Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título

9, parte 2, libro 2)

- Directiva presidencial 02 de 2019 - Simplificación de la interacción digital entre los ciudadanos y el Estado
- Ley 1712 de 2014 - Transparencia y Acceso a la Información Pública
- Decreto 415 de 2016 (Compilado en el Título 35, parte 2, libro 2 del Decreto No. 1083 de 2015) - Lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones
- Decreto 1413 de 2017 (Título 17, parte 2, libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015 - Reglamenta la prestación de los Servicios Ciudadanos Digitales

5. ÁMBITO DE APLICACIÓN

Entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas. La implementación de la Política de Gobierno Digital en las Ramas Legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en los artículos 113 y 209 de la Constitución Política (Art. 2.2.9.1.1.2. - Decreto 1078 de 2015).

5.1 Lineamientos generales para la implementación

En el orden nacional, en los Comités Sectoriales de Gestión y Desempeño se darán las directrices para su implementación, en el Comité Institucional de Gestión y Desempeño se debe articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política. Para ello, se debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área transversal que haga parte de la Alta Dirección

La política de Gobierno Digital se implementa a través de dos líneas de acción que orientan su desarrollo: TIC para el Estado y TIC para la Sociedad; así como de tres habilitadores transversales, que son los elementos que proporcionan la base de la política: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. A continuación, se define cada uno de estos elementos:

5.1 Políticas de acceso a recursos y servicios de TI y facilidades tecnológicas por parte de los grupos de interés, comprende políticas relacionadas con el hardware, software, acceso a recursos y servicios de TI, y uso de redes y telecomunicaciones.

5.2 Políticas de Componentes de Información y bases de datos: las cuales establecen lineamientos sobre la gestión de componentes de información, la calidad de éstos. Además, define directrices sobre la creación y acceso a bases de datos, la conservación y respaldo de la información almacenada en éstas, también la configuración y administración de las cuentas de bases de datos y el uso de privilegios, entre otras.

5.3 Políticas de Continuidad de TI, definen lineamientos que permitan la Oficina de Tecnologías y Sistemas de Información actuar en los eventos que se presenten que puedan afectar la operación de TI del IDESAN, así como su prevención.

5.4 Políticas de Seguridad de la Información, tiene por objeto: establecer los lineamientos necesarios, con el fin de fortalecer la gestión de seguridad y privacidad de la información del IDESAN, enmarcados en la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la identificación y valoración de los riesgos asociados a ella, propendiendo por la protección de su confidencialidad, integridad, disponibilidad, privacidad, continuidad, y autenticidad. En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades.

Con la aplicación de esta política se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital.

Marco Normativo

- Acuerdo 08 de 2019
- Ley 1928 de 2018
- Acuerdo 02 de 2018
- CONPES 3854 de 2016
- Decreto 1078 de 2015
- Ley 1712 de 2014
- Transparencia y Acceso a la Información Pública

- Ley estatutaria 1581 del 2012
- Decreto 103 de 2015

6. ESTRATEGIA: PORTAFOLIO DE INICIATIVAS PROYECTOS Y HOJA DE RUTA

Objetivo Estratégico institucional ***FORTALECER TECNICA ADMINISTRATIVA Y FINANCIERAMENTE AL INSTITUTO, PARA AFRONTAR LOS RETOS COMO EL INFI AL SERVICIO DE NUESTRO DEPARTAMENTO.***

6.1 SITUACIÓN ACTUAL

6.1.1 INFRAESTRUCTURA DIGITAL

Descripción de la plataforma tecnológica sobre la cual operan las actividades supervisadas, considerando elementos tales como:

6.1.2 EQUIPOS CENTRALES

El instituto financiero para el desarrollo de Santander – IDESAN ha venido actualizando la plataforma tecnológica en su totalidad; los funcionarios cuentan con equipos modernos y acordes a las exigencias de los diferentes procesos.

CANTIDAD	DESCRIPCION	UTILIDAD
1	**Servidor**	Actualmente se trabaja en un ambiente Microsoft Windows Server 2012 R2, todas las oficinas del Instituto se encuentran en red interna con una infraestructura de cableado estructurado de categoría 7ª.
37	**Computadores**	Equipos disponibles para los funcionarios del instituto.
14	**Portátiles**	Equipos disponibles para los funcionarios del instituto.
12	**Impresoras inyección de tinta, laser Jet.**	Equipos disponibles para los funcionarios del instituto.

2	**Impresoras de matriz de punto carro ancho**	Equipos disponibles para los funcionarios del instituto.

Los equipos de cómputo cuentan con las siguientes especificaciones técnicas y se encuentran distribuidos de la siguiente manera:

SERVIDOR					
No.	**UBICACIÓN**	**DISCO DURO**	**MEMORIA**	**PROCESADOR**	**BOARD**
1	**SERVIDOR HP (NUEVO)**	10 TB	8 GB	Intel® Xeon® CPU ES-240F – 2.20 GHZ	PROLIANT ML 350 GEN 8
COMPUTADORES DE ESCRITORIO					
No.	**UBICACIÓN**	**DISCO DURO**	**MEMORIA**	**PROCESADOR**	
1	**SISTEMAS**	1 TB	4 GB	INTEL CORE i5 (TODO EN UNO)	
2	**SERVIDOR VIEJO**	250 GB	4 GB	INTEL XEON E5-2407	
3	**PLANEACION-bodega**	250 GB	2 GB	INTEL CORE 2 DUO – 2.93 GHZ	
4	**ARCHIVO**	500 GB	4 GB	INTEL CORE i3	
5	**AUX-ARCHIVO**	300 GB	4 GB	INTEL CORE 2 DUO – 2.8 GHZ	
6	**CALIDAD**	SSD 240 GB	4 GB	INTEL CORE i5	
7	**CALIDAD**	1 TB	8 GB	INTEL Corel i5-7400 Dual-Core	
8	**CARTERA 1**	500 GB	4 GB	INTEL CORE i5	
9	**CARTERA 2-bodega**	500 GB	2 GB	INTEL PENTIUM DUAL	
10	**CARTERA 2**	1 TB	8 GB	INTEL Corel i5-7400 Dual-Core	
11	**CONVENIOS**	500 GB	4 GB	INTEL CORE i5	
12	**AUX-CONVENIOS**	500 GB	4 GB	INTEL CORE i3	
13	**TESORERO**	1 TB	4 GB	INTEL CORE i5 (TODO EN UNO)	
14	**TESORERIA 4**	320 GB	4 GB	INTEL CORE 2 DUO	

15	**TESORERIA 1**	1 TB	8 GB	INTEL Corel i5-7400 Dual-Core
16	**TESORERIA 3**	320 GB	4 GB	INTEL CORE i5

17	**TESORERIA 2**	SSD 240 GB	4 GB	INTEL CORE 2 DUO
18	**SEC-GERENCIA**	500 GB	4 GB	INTEL CORE i5
19	**FINANCIERO**	1 TB	4 GB	INTEL CORE i5 (TODO EN UNO)
20	**ESTUDIO-FRO-**	250 GB	4 GB	INTEL DUAL CORE
21	**ESTUDIO FINANCIERO**	1 TB	8 GB	INTEL Corel i5-7400 Dual-Core
22	**SEGUIMIENTO-FRO**	500 GB	4 GB	INTEL CORE i5
23	**APOYO-FRO**	250 GB	4 GB	INTEL CORE 2 DUO
24	**COMERCIAL**	500 GB	4 GB	INTEL CORE I5
25	**CREDITOS**	500 GB	4 GB	INTEL CORE I5
26	**APOYO-COMERCIAL**	1 TB	4 GB	INTEL CORE I5 (TODO EN UNO)
27	**RIESGOS 1**	500 GB	4 GB	INTEL CORE i5
28	**RIESGOS 2**	1TB	4 GB	INTEL CORE i5 (TODO EN UNO)
29	**ADMINISTRATIVO**	500 GB	4 GB	INTEL CORE i5
30	**CONTABILIDAD**	240 GB-solido	4 GB	INTEL CORE i5
31	**JURIDICO**	240 GB-solido	4 GB	INTEL CORE i5
32	**AUX-JURIDICO**	500 GB	4 GB	INTEL CORE i3
33	**APOYO-JURIDICO**	500 GB	4 GB	INTEL CORE i3
34	**CONTROL INTERNO- apoyo**	500 GB	4 GB	INTEL CORE i3

35	**CONTROL INTERNO**	1 TB	8 GB	INTEL Corel i5-7400 Dual-Core
36	**PLANEACION**	1 TB	8 GB	INTEL Corel i5-7400 Dual-Core

37	**CONTROL INTERNO**	240 GB-solido	4 GB	INTEL CORE i5
PORTATILES				
01	**ABOGADA-CONVENIOS**	500 TB	4 GB	INTEL CORE i5
02	**GERENCIA**	500 GB	4 GB	INTEL CORE i5
03	**COMERCIAL -**	250 GB	2 GB	AMD E-350
04	**JURIDICO**	500 GB	4 GB	INTEL DUAL i5
05	**JURIDICA P-1-**	500 GB	4 GB	INTEL CORE i3
06	**COMERCIAL P-1-**	500 GB	4 GB	INTEL CORE I5
07	**PRENSA**	1 TB	8 GB	INTEL CORE i7
08	**RIESGOS 3**	500 GB	4 GB	INTEL CORE i5
09	**JURIDICO P-2-**	500 GB	2 GB	AMD E-450
10	**FINANCIERO-apoyo**	250 GB	2 GB	AMD E-450
11	**FINANCIERO Y ADTVO**	500 GB	4 GB	INTEL CORE I5
12	**SEC-GERENCIA**	1 TB	8 GB	INTEL CORE I5-7200U
13	**JURIDICA**	1 TB	8GB	INTEL CORE I5-7200U
14	**COMERCIAL**	1TB	8GB	INTEL CORE I5-7200U

6.1.3 IMPRESORAS Y SCANNER DEL INSTITUTO

DEPENDENCIA	IMPRESORA	No. INVENTARIO	SCANNER	No. INVENTARIO
SECRETARIA GERENCIA	EPSON L 575	0924	HP SCANJET PRO 4500 FN1	0940
FRA. Y ADTIVA	EPSON L 575	1004		
TESORERIA	HP Laserjet M1132 MFP (planeación)	1070	EPSON GT-555	1252
	EPSON L575	0852		
	HP laserJet M1132 MFP (jurídica)	0954		
CONVENIOS	HP Laserjet 1022	0891	HP SCANJET 63110 AVISION AD240U	2309
	HP Laserjet 1022	3764		
	EPSON L575	0930		1017
	EPSON FX-2190	3742		
CARTERA1	EPSON L3110	181	HP SCANJET G2710	1499
PLANEACIÓN – CALIDAD- RIESGOS	HP Laserjet 1022	3819	CANON DR-3010C PANASONIC -KV-S1057C	1272 1013
	EPSON L-355	1509		
	HP Laserjet P2014n (tesorería)	0880		
	EPSON L575	0958		
	EPSON L 575	0999		
	EPSON L 575	0997		
SISTEMAS	HP Laserjet M1132 MFP	1028		
	EPSON FX-890 II	1010		
ASESOR COMERCIAL	EPSON L575	0931		
	HP CP1215	1671		

CRÉDITOS	EPSON L355	1448	AVISION AD240U	1015
ADMINISTRATIVO Y CONTABILIDAD – APOYO FINANCIERO	EPSON L575	1003	CANON DR-3010C	1094
	EPSON L575	0917		
	HP Laserjet 1022 HP Laserjet L565,	3822 3986		
JURÍDICA	HP Laserjet 1022	3751	HP SCANJET PRO 4500 FN1	0957
			AVISION AD240U	1016
	HP Laserjet M1120 MFP (tesorería)	1276		
	HP Laserjet 1022 (planeación)	0854		
	HP Laserjet P1102W	1366		
GERENCIA	HP Laserjet P1006	1246		
CONTROL INTERNO	HP Laserjet 1022 EPSON L 575	2341 1006	AVISION AD240U	1014

7. SISTEMAS OPERATIVOS:

El instituto cuenta con diferentes sistemas operativos ya que gestiona los procesos básicos del sistema, se trabaja con las diferentes versiones de WINDOWS (Windows XP, Windows Vista, Windows 7, Windows 9, Windows 10…) propiedad de la empresa Microsoft que es privativo (de pago), incluyendo el paquete ofimático de Microsoft Office (Office 2003, Office 2007, Office 2010…). En el servidor se trabaja en un ambiente Microsoft Windows Server 2012 R2, todas las oficinas del Instituto se encuentran en red interna con una infraestructura de cableado estructurado 7ª.

7.1 RELACIÓN DE EQUIPOS DE CÓMPUTO CON SU RESPECTIVA LICENCIA:

No.	EQUIPO	SOFTWARE	UBICACIÓN
1	PC	Windows 7 Pro OA – Office Profesional 2007	Tesorería 4
2	PC	Windows 7 Pro OA – Office Profesional 2007	Tesorería 2
3	PC	Windows 7 Pro OA – Office Profesional 2007	Tesorería 3
4	PC	Windows 7 Pro OA – Office Profesional 2007	Aux Archivo
5	PC	Windows 7-8 – Office Hogar y Empresas 2013	Apoyo Financiero
6	PC	Windows 7-8 – Office Enterprise 2007	Sec-Gerencia
7	PC	Windows 7-8 – Office Professional 2007	Administrativo
8	PC	Windows 7-8 – Office Professional 2007	Créditos
9	PC	Windows 7-8 – Office Professional 2007	Riesgos 1
10	PC	Windows 7-8 – Office Hogar y Empresas 2013	Convenios
11	Servidor (nuevo)	Windows Server Std 2012 R2	Sistemas
12	PC (servidor viejo)	Windows Small Business Server 2003	Sistemas
13	PC	Windows 7 – Office Hogar y pequeña empresa 2010	Control Interno
14	PC	Windows 7 – OfficeHogar y pequeñaempresa 2010	Apoyo-Jurídico
15	PC	Windows 7 – OfficeHogar y pequeñaempresa 2010	Aux-Jurídico
16	PC	Windows 7 – OfficeHogar y pequeñaempresa 2010	Archivo

17	PC	Windows 7 – OfficeHogar y pequeñaempresa 2010	Aux- Convenios
18	PC	Windows Vista Business OA – Office Profesional 2007	Estudio-Financiero - practicante
19	PC	Windows XP Profesional – Office Enterprise 2007	Cartera 2 (bodega)
20	PC	Windows XP Profesional – Office Enterprise 2007	Planeación (bodega)
21	PC	Windows 8.1 Pro - Office Hogar y empresas 2016	Seguimiento Financiero
22	PC	Windows 8.1 Pro - Office Hogar y empresas 2016	Asesor Comercial
23	PC	Windows 8.1 Pro - Office Hogar y empresas 2016	Cartera 1
24	PC	Windows 8.1 Pro - Office Hogar y empresas 2016	Control Interno (apoyo)
25	PC	Windows 8.1 Pro - Office Hogar y empresas 2016	Contabilidad
26	PC	Windows 8.1 Pro - Office Hogar y empresas 2016	Jurídica
27	PC	Windows 8.1 Pro - Office Hogar y empresas 2016	Calidad – Alejandro
28	TODO EN UNO	Windows 10 Pro – Office home and busines 2016.	Sistemas
29	TODO EN UNO	Windows 10 Pro – Office home and busines 2016.	Apoyo Comercial
30	TODO EN UNO	Windows 10 Pro – Office home and busines 2016.	Riesgos 2
31	TODO EN UNO	Windows 10 Pro – Office home and busines 2016.	Financiero y Administrativo
32	TODO EN UNO	Windows 10 Pro – Office home and busines 2016.	Tesorero
33	TODO EN UNO	Windows 10 Pro – Office home and busines 2016.	Tesorería 1
34	TODO EN UNO	Windows 10 Pro – Office home and busines 2016.	Planeación
35	TODO EN UNO	Windows 10 Pro – Office home and busines 2016.	Cartera 2

36	TODO EN UNO	Windows 10 Pro – Office home and busines 2016.	Calidad - Daniel
37	TODO EN UNO	Windows 10 Pro – Office home and busines 2016.	Control Interno
38	TODO EN UNO	Windows 10 Pro – Office home and busines 2016.	Estudio Financiero
1	Portátil	Windows 10 Pro – Office home and busines 2016.	Riesgos 3
2	Portátil	Windows 10 Pro – Office home and busines 2016.	Abogada Convenios
3	Portátil	Windows 10 Pro – Office home and busines 2016.	Comercial P-2 – camilo
4	Portátil	Windows 10 Pro – Office home and busines 2016.	Financiero y Administrativo
5	Portátil	Windows 10 Pro – Office home and busines 2016.	Gerencia
6	Portátil	Office home and busines 2016.	Prensa
7	Portátil	Windows 7 – Office Hogar y pequeña empresa 2010	Jurídico P-1- Jorge
8	Portátil	Windows 7 – OfficeHogar y pequeñaempresa 2010	Jurídica P-1 – Milena A cene
9	Portátil	Windows 7 starter – Office 2010	Jurídica - Willian
10	Portátil	Windows 7 Pro – Office 2007	Financiero - nancy
11	Portátil	Windows 7 pro – Office 2007	Comercial – pequeño
12	Portátil	Windows 10 Pro – Office home and busines 2016.	Sec-gerencia
13	Portátil	Windows 10 Pro – Office home and busines 2016.	Juridica- sebastian
14	Portátil	Windows 10 Pro – Office home and busines 2016.	Comercial - humberto

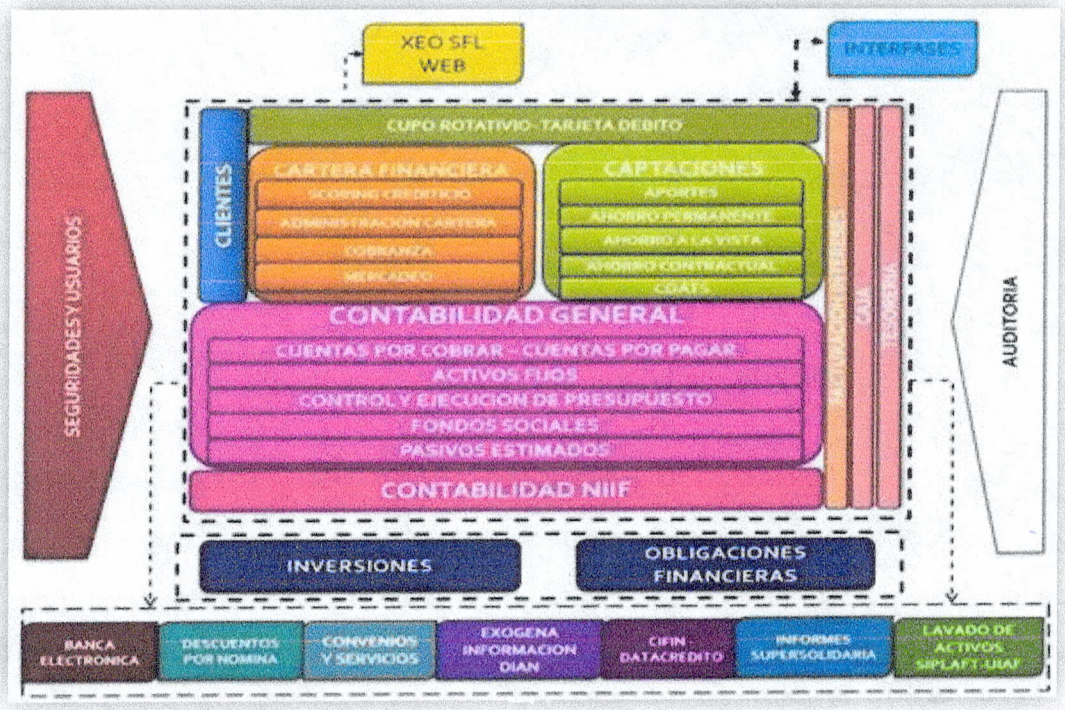
8. SISTEMA DE ADMINISTRACIÓN DE BASES DE DATOS

8.1 Sistema Financiero XEO

Es un sistema de información administrativo y financiero para apoyar los procesos misionales de Entidades de Crédito y Financieras, Cooperativas, Fondos de Empleados, Entidades de Microfinanzas, Fundaciones e Institutos Financieros Gubernamentales "INFIS".

Actualmente, el Instituto es usuario del software financiero XEO y el titular de los derechos de autor son exclusivos de la Empresa TECNOINFORMÁTICA S.A.S. que se cuenta con el software XEO y Software SIIARE donde la empresa ofrece al Instituto configuración, consultoría, soporte correctivo, evolutivo, actualizaciones, y capacitación al personal en el manejo de los aplicativos, mantenimiento y revisión del Aplicativo Xeo Gestión Oficial: Contabilidad Oficial, Activos Fijos, Presupuesto Oficial, Cartera Financiera y ahorros, Central Riesgo de Cartera – Cifin, Descuentos por Libranza, Convenios, Gerencial de Contabilidad, Riesgo de Liquidez – Formato 458, información exógena DIAN formatos 1001, 1003, 1007, 1008, 1009, 1010, 1011 y 1012, NIIF, Informes Superfinanciera formatos 509, 510, 511, 512, 513, 514 y 515, Flujo de trabajo en fábrica de crédito, Pago y aplicación de abonos en línea mediante botón de pagos y servicio de mantenimiento para el software Web SIIARE de administración del riesgo empresarial: SARO, SARLAFT, SARC, SARM y SARL. Con esta empresa se adquirió la licencia de uso por tiempo ilimitado del software ya que son los únicos desarrolladores del Software Financiero XEO.

.



8.2 Lenguaje de Programación:

El sistema opera en un lenguaje de programación PowerBuilder y trabaja en una base de datos Sybase en una plataforma bajo ambiente Windows y es un sistema multiusuario y todos los módulos trabajan en línea, es decir, los módulos de cartera, ahorros e inversiones y presupuesto comunican directamente al módulo de contabilidad, por lo tanto, no requiere del proceso de comunicación pero si de un proceso de actualización, el sistema de información del Instituto se encuentra instalado en un servidor HP Proliant ML 350, con un sistema operativo Microsoft Windows Server 2008-2012. El Software SIIARE opera en un lenguaje de programación ASP.NET MVC 5.NET Core C#, Entity Framework 6 HTML 5 CS 3 JavaScript.NET Framework 4.5.2 Bootstrap y trabaja e una base de datos SQL Server 64 bits 2014.

8.3 Software Administración Documental – DOCUADMIN.

Es un Sistema de Administración y Gestión de Documentos que ha sido creado por el equipo de Desarrollo de Software de la firma Numérica Ltda. Que organiza documentos

digitales en una base de datos de una manera jerárquica y organizada, lo cual facilita la exploración y visualización de los mismos. Además, cuenta con un eficiente buscador que localiza cualquier documento solamente conociendo algún índice de o de losdocumentos de interés. Se realizó de acuerdo a las normas del Archivo General de la nación. No solo para gestionar información sino para servir de soporte al proceso administrativo de las organizaciones a través de un sofisticado sistema de alertas, controlde vencimiento de documentos, de versiones y de flujos documentales.

9. PRINCIPALES CARACTERÍSTICAS DEL PETI

9.1 Arquitectura

- ✓ Arquitectura cliente – servidor
- ✓ Servidor de base de datos independiente del repositorio de imágenes
- ✓ Preconfigurado con la base de datos PostgreSQL. (Robusta y Libre)
- ✓ Módulo de consultas web
- ✓ Esquema de licencias flotantes (Se puede instalar DocuAdmin® en un número ilimitado de equipos, y el servidor controla el número máximo de usuarios que estén conectados al mismo tiempo de acuerdo a la cantidad de licencias adquiridas)

9.2 Organización

- ✓ Árbol de Secciones y Sub-Secciones configurable por el cliente sin límite de niveles, ajustable a cualquier estructura organizacional
- ✓ Manejo de Roles de usuarios independientes de acuerdo a la estructura organizacional

9.3 Series Documentales

- ✓ Tabla de Series Documentales General para toda la organización, pero asociables por sección
- ✓ Manejo de subseries sin límite de niveles
- ✓ Manejos de tipologías por series documentales: Facilita la organización de tipos documentales dentro de una serie.
- ✓ Índices personalizados para cada serie documental o tipología
- ✓ Despliegue de lista en árbol (padre - hijo) para manejo de jerarquía de series y tipologías
- ✓ Administración y Gestión de las tablas de retención documental
- ✓ Localización de documentos de acuerdo a la TRD
- ✓ Control de índices únicos dentro de la serie
- ✓ Manejo de listas de valores predefinidas (para valores de un metadato que estén

restringidos a un conjunto limitado de opciones, evita la digitalización manual, ya que el valor se escoge de la lista desplegable)

9.4 Navegación

- ✓ Navegación intuitiva a través del árbol de secciones, al estilo del explorador de Windows
- ✓ Búsquedas rápidas con cualquier texto de cualquier índice
- ✓ Búsquedas avanzadas con combinación de criterios
- ✓ Visualización directa de imágenes asociadas al documento

9.5 Gestión De Documentos

- ✓ Flujos asignables a los documentos
- ✓ Alertas asignables a los documentos. Ej. Vencimientos
- ✓ Manejo de múltiples versiones de un documento
- ✓ Anotaciones sobre los documentos
- ✓ Conexión directa con el escáner para digitalización
- ✓ Asociación de cualquier tipo de archivo digital

9.6 Automatización De Documentos

- ✓ Procesamiento automático de índices con OCR a partir de las imágenes de los documentos de manera individual o por lotes
- ✓ Procesamiento automático de resúmenes de los documentos a través del OCR aplicado a toda la imagen del documento
- ✓ Importación de metadatos y creación de documentos a partir de archivos de Excel (CSV)

9.7 Seguridad

- ✓ Asignación de permisos flexible y detallada, por rol, serie documental y sección
- ✓ Encriptación de claves de usuario con algoritmo MD5 de 128 bits

9.8 Administración

- ✓ Administrador de usuarios, roles y permisos
- ✓ Administrador de series, subseries tipologías y tablas de retención documental
- ✓ Administrador del repositorio de base de datos
- ✓ Administrador de Auditoría

9.9 Informes

- ✓ Estadísticas generales
- ✓ Estadísticas de Flujos
- ✓ Informes de Alertas
- ✓ Gestión de Tablas de Retención Documental
- ✓ Configuración de permisos

10. PORTAL WEB

El instituto a la fecha cuenta con una página web www.idesan.gov.co totalmente estructurada llevando a cabo el cumplimiento de los lineamientos de Gobierno Digital, manejando una dinámica propia de las Tecnologías de la Información y la Comunicación. Donde asume un proceso gradual, evolutivo, coordinado y colectivo asumido por todas las entidades de Administración Pública.

El contenido del Portal Web sobre Información en Línea es el siguiente:

CRITERIO	OBSERVACIONES
Nosotros	
Quienes Somos	Información general del instituto financiero para el desarrollo de Santander - IDESAN
Dependencias	Se muestran todas las dependencias que contiene IDESAN.
S.G.C – Meci	Información referente al Sistema de Gestión de Calidad y al Modelo Estándar de Control Interno que maneja el instituto.
Idesan Para niños	Un mini Portal Web especial para los niños; se muestra la información de una manera didacta.
Informes	Actualiza al usuario de los diferentes procesos internos del Instituto.
Clientes	Muestra el portafolio de servicios al cual va dirigido el Instituto.
Presupuesto	Publicación de presupuesto aprobado de acuerdo con las normas vigentes aplicadas por el instituto.
Normatividad	
Nacionales	
Departamentales	
En el Instituto	

Centro de Evacuación	Publicación de toda la información referente a la normatividad que rige el Instituto. La información se

Código buen gobierno	encuentra actualizada, organizada por temática con el fin de que el usuario pueda descargar dicha información
Estructura y Documentación	
Planes y proyectos	
Planes y programas	Se publica las políticas, planes, líneas estratégicas, proyectos y programas especiales, planes de acción y mejoramiento que se ejecutan en cada vigencia.
Proyectos especiales	
Planes de mejoramientos	
Plan de acción	
Servicios	
Captación	Se visualiza la sección de servicios del instituto, donde se proporciona un listado de cada servicio ofrecido para que la comunidad pueda hacer uso de él.
Líneas de Crédito	
Formatos de Crédito	
Tramites	
Otros Servicios	
Servicios de Información	
Noticias	Se informa a la comunidad de los hechos más importantes del instituto de una manera actualizada.
Trabaja con Nosotros	Publicación de empleo vigente, perfil requerido, periodo de la oferta y datos de contacto.
Galería	Se muestras imágenes actualizadas de eventos, reuniones o hechos importantes que destaquen el instituto.
Consulta en línea	Hay un chat de consulta en línea para resolver dudas e inquietudes sobre el Instituto.
Localización física	Se publica los datos de contacto para cuando el usuario necesite alguna información del Instituto.
Teléfonos	
Correo electrónico de contacto	
Horario de Atención	

Portal Web maneja los siguientes estándares de navegación:

CRITERIOS	OBSERVACIONES
Estándares de Presentación	
Identidad visual	Se muestra una identidad gráfica y visual con la nueva imagen institucional; para que sea un portal atractivo, útil y actual tanto para funcionarios como para la comunidad en general.
Enlace al Portal del Sistema Electrónico para la Contratación Publica	Al hacer clic en el enlace del portal de una vez los direcciona a la página web https://www.contratos.gov.co
Estándares de Funcionalidad	
Acceso a la página de Inicio	Se incluye el acceso directo a la página de Inicio para un fácil acceso a cualquier otra página del Portal Web
Mapa del Sitio	Contiene en la página de Inicio el acceso a Mapa del Sitio para acceder a todas las secciones del Portal Web.
Correo Institucional	Enlaza al funcionario directamente al correo de Gmail.
Cobertura Geográfica	Hace el enlace a la página web http://sigotn.igac.gov.co/sigotn/

11. RED DE COMUNICACIONES

Se cuenta con un cableado estructurado y su correspondiente soporte eléctrico, el cual son 47 puntos de red lógicos categoría 7ª certificados, que están distribuidos y administrados por un Rack principal ubicado en el tercer piso del IDESAN en la oficina de Sistemas, interconectados por un **SWITCH ADMINISTRABLE PRINCIPAL (TIPO CORE)**. Estos puntos están distribuidos en diferentes áreas asistenciales y administrativas, de acuerdo a las necesidades que se presenten en las mismas.

La Entidad cuenta con un (1) Servidor (en ambiente Microsoft Windows Server 2012 R2), treinta y siete (37) Computadoras (Terminales Inteligentes) y catorce (14) portátiles. Treinta (30) impresoras inyección de tinta y Láser Jet y dos (2) impresora de matriz de punto.

La Entidad cuenta con un servicio de internet con un canal Wifi dedicado de 20 megas simétrico, especificaciones de canal dedicado simétrico 1:1.

11.1 CANALES MEDIANTE LOS CUALES SE PRESTAN LOS SERVICIOS INDICANDO SI SON PROPIOS O SE TIENE CONTRATO CON UN TERCERO

El Instituto Financiero para el Desarrollo de Santander - IDESAN en la vigencia 2021 cuenta con contratos con terceros que son los siguientes:

No. Contrato: J-026	Fecha: enero 25 de 2022
Contratista:	TECNOINFORMATICA S.A.S NIT: 800.068.685-1
Objeto:	Prestar el servicio de mantenimiento, configuración, consultoría, soporte correctivo, evolutivo, actualizaciones, capacitación al personal, revisión y desarrollo adicional permanente al Aplicativo XEO INFIS (Clientes, Contabilidad Oficial, Cartera Financiera, Ahorros, Convenios, NIIF, Obligaciones Financieras, Inversiones, Activos Fijos, Presupuesto Oficial, Central Riesgo de Cartera – Cifin, Descuentos por Libranza, Gerencial de Contabilidad, Riesgo de Liquidez – Formato 458, información exógena DIAN formatos 1001, 1003, 1007, 1008, 1009, 1010, 1011 y 1012, Informes Superfinanciera formatos 509, 510, 511, 512, 513, 514 y 515, Flujo de trabajo en fábrica de crédito, activación de plataforma SFL Pago y aplicación de abonos en línea mediante botón de pagos y Servicio de Mantenimiento para el software Web SIIARE de administración del riesgo empresarial (SARO, SARLAFT, SARC, SARM y SARL) con que cuenta licenciado IDESAN.
Valor:	SETENTA MILLONES DE PESOS $70.000.000, oo MCTE.
Termino de Duración:	28 de diciembre de 2022.

No. Contrato: J-025	**Fecha: enero 29 de 2021**
Contratista:	COINSA S.A.S 800.143.512-5
Objeto:	RENOVACIÓN LICENCIA ANTIVIRUS ESET ENDPOINT SECURITY: EAV-0242529964, PARA USUARIO, SERVIDOR, LICENCIA POR 3 AÑOS. PARA 60 LICENCIAS INCLUIDO SERVIDOR. FUNCIONES PRINCIPALES: ANTIVIRUS, ANISPYWARE, FIREWALL, ANTISPAM, CONTROL PRENTAL. Derecho a instalación y soporte técnico presencial y demás componentes que el fabricante llegue a liberar durante la vigencia de la licencia.
Valor:	CINCO MILLONES NOVECIENTOS CATORCE MIL CUATROCIENTOS SETENTA Y SIETE PESOS $5.914.477 MCTE.
Termino de Duración:	Cinco (5) días hábiles, a partir de la suscripción del acta de inicio para la instalación , pero el licenciamiento es hasta enero de 2024.

No. Contrato: J-031	**Fecha: enero 27 de 2022.**
Contratista:	EDWIN ORLANDO CORREA RAMIREZ **C.C. 91.273.895**
Objeto:	EL CONTRATISTA DE MANERA AUTONOMA E INDEPENDIENTE SE OBLIGA CON EL IDESAN A PRESTAR LOS SERVICIOS PROFESIONALES Y DE APOYO A LA GESTION EN EL AREA DE SISTEMAS.
Valor:	QUINCE MILLONES DE PESOS $15.000.000 MCTE.
Termino de Duración:	Cinco (05) meses.

11.2 CENTRO DE CÓMPUTO PRINCIPAL Y DE CONTINGENCIA INDICANDO LOS CONTROLES DE SEGURIDAD FÍSICA Y DE AMBIENTE.

CONTROLES DE SEGURIDAD LÓGICA A NIVEL DE SISTEMA OPERATIVO Y BASE DE DATOS:

11.2.1 Controles de Acceso

Los controles de acceso manejados dentro del Instituto Financiero para el Desarrollo de Santander - IDESAN en protección a los sistemas de información, a las Bases de Datos o demás aplicativos, ayudan a proteger los sistemas operativos, la red, sistemas de aplicación y demás software, manteniendo la integridad de la información en cuestión de procesos y accesos permitidos por los usuarios con el fin de resguardar información valiosa.

11.2.2 Identificación y autenticación:

A cada funcionario se le asigna un usuario brindando los permisos de lectura y escritura para visualización de contenidos, modificación o ejecución de archivos conectados en red. Incluyendo el Sistema Financiero XEO – Software SIIARE y el Software Administración Documental DOCUADMIN se le asigna un usuario dependiendo del perfil a trabajar.

11.2.3 Identificación: Todos los usuarios son asignados por el servidor, ejemplo: sistemas. IDESAN. local. Los usuarios de XEO, SIIARE y DOCUADMIN son asignados directamente del Software.

11.2.4 Autenticación: Todos los usuarios deben validar su identificación mediante la contraseña (clave) para acceder al sistema. Las claves deben tener las siguientes características:

- Debe tener de 6 a 8 dígitos.
- Debe incluir Mayúsculas, números y caracteres.
- Solo el usuario debe escoger la contraseña, no el sistema.
- No utilizar nombre de familiares u otros datos personales.
- No debe estar en exhibición pública y menos pegarla en el monitor o escritorio.
- La contraseña se debe cambiar periódicamente.

11.2.5 Roles:

- **Sistema Financiero XEO**

A cada funcionario se le asigna un perfil o rol usuario según el acceso que requiera.

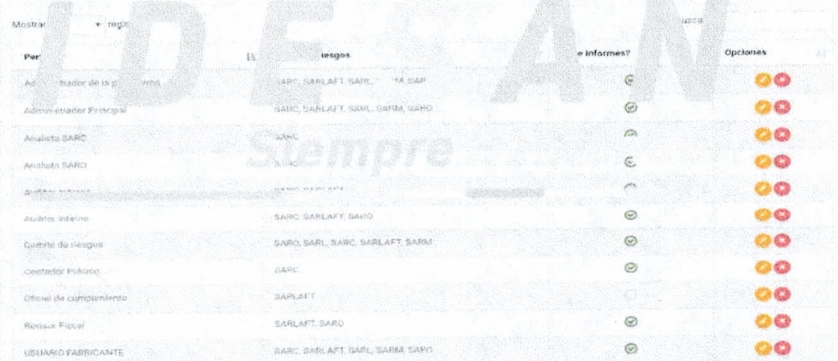
Los roles son los siguientes:

- Tesorería Caja
- Tesorería jefe
- Activos Fijos
- Control Interno
- Auxiliar Contabilidad
- Tesorería Caja2
- Cartera jefe
- Practicante Contabilidad
- Practicante Asesor Comercial
- Administrador
- Técnico (E)
- Sistemas
- Contador Contratista
- Convenios Apoyo

Existen restricciones de permisos de acceso no todos los usuarios tienen derecho a ejecutar, grabar, borrar, listar, extraer o modificar información del Software.

❖ **Software SIIARE Web**

A cada funcionario se le asigna un perfil o rol usuario según el acceso que requiera. Los perfiles son los siguientes:



Existen restricciones de permisos de acceso no todos los usuarios tienen derecho a ejecutar, grabar, borrar, listar, extraer o modificar información del Software.

❖ **Software Administración Documental – DOCUADMIN**

La creación de perfiles, Usuarios, Secciones, Subsecciones, Series Documentales y demás labores administrativas están a cargo de un usuario especial que pertenece a la sección Administrador. Esta sección ya viene predefinida en DOCUADMIN y a él

pertenecen todos los usuarios autorizados para ejecutar tareas administrativas, sobre el control total de DOCUADMIN.

11.2.6 Limitación a los servicios:

Las limitaciones a los servicios se registran directamente en el servidor, brindando permisos de acceso necesario con un trabajo simultáneo en todos los usuarios asignados por el sistema, que en su totalidad son 25 registrados, pero en cada equipo de cómputo pueden ingresar más de un usuario.

En el Sistema Financiero XEO, SIIARE web y el Software Administración Documental DOCUADMIN son aplicativos que se pueden trabajar simultáneamente sin limitar número de usuarios.

11.2.7 Modalidad de Acceso

Se utiliza algunos modos de acceso que permite al usuario manejar los recursos y la información existente tanto en el servidor como en los dos softwares utilizados dentro del Instituto.

❖ **Servidor:**

- Lectura: El usuario puede únicamente leer o visualizar información, pero no se puede alterar.
- Escritura: Este tipo de acceso permite agregar datos, modificar o borrar.

❖ **Sistema Financiero XEO, SIIARE web:**

- Ejecutar: Otorga al usuario el permiso de ejecutar la información que desee manejar
- Grabar: otorga al usuario el permiso de grabar los cambios o información necesaria manejada en el software.
- Borrar: Permite al usuario eliminar archivos o campos de datos del software.
- Listar: Permite que el usuario vea la información de otra manera.
- Extraer: Permite al usuario descargar la información manejada.
- Modificar: Permite al usuario hacer modificaciones o cambios en algún archivo o campo de datos.

❖ **Software Administración Documental - DOCUADMIN:**

- Explorar: El usuario solo puede ver, consultar y hacer búsquedas sobre los metadatos de los documentos, pero no puede acceder al documento digital.
- Visualizar: Además de Explorar, al usuario le está permitido acceder al documento digital.

- Escribir: Contiene al anterior, pero, además, el usuario puede editar, eliminar y creardocumentos.

11.2.8 Administración

Una vez establecidos los controles de acceso sobre los sistemas de información del instituto se realizan medidas de implementación, seguimiento, pruebas y modificaciones sobre los accesos de los usuarios al sistema.

12. ADMINISTRACIÓN DEL PERSONAL Y USUARIOS:

12.1 Definición de Puestos: A los usuarios del Instituto se le otorgan las funciones necesarias según su cargo laboral, con los debidos permisos de acceso a los diferentes sistemas de información manejados internamente. Cada dependencia maneja los siguientes cargos:

- **Tesorería:** Tesorería Caja, Tesorería Jefe, Tesorería Caja2.
- **Planeación:** Activos Fijos
- **Control Interno:** Control Interno
- **Contabilidad:** Auxiliar Contabilidad, Practicante Contabilidad, Contador Contratista
- **Convenios:** Convenios Apoyo,
- **Cartera:** Cartera Jefe
- **Sistemas:** Técnico (E), Sistemas, Administrador
- **Financiero y Administrativo:** Administrador

12.2 Determinación de la sensibilidad del puesto: Todos los accesos son controlados por el administrador del sistema de información, cada usuario maneja permisos según su actividad para que no existan fraudes, alteración de procesos y visualización de información confidencial.

12.3 Elección de la persona para cada puesto: Los funcionarios administrativos del Instituto cumplen con la experiencia laboral y conocimientos técnicos necesarios para asumir cada cargo, ya que se hace un análisis de la hoja de vida cerciorándose que sean los datos correctos.

Para el Sistemas Financiero XEO y el Software Administración Documental DOCUADMIN se les asigna un perfil cuando el Supervisor lo requiera indicando las tareas a realizar.

12.4 Entrenamiento Inicial y Continuo del empleado: Se realizan capacitaciones internas y externas sobre los sistemas de información del instituto.

Para los contratistas se les realiza una inducción y capacitación respectiva sobre el manejo del Sistema Financiero XEO – Software SIIARE Web y del Software Administración Documental DOCUADMIN.

12.5 Actualizaciones del sistema y aplicaciones

Se realizan mantenimientos correctivos periódicamente con el fin de ir actualizando los sistemas operativos de los equipos de cómputo, la mayoría de aplicaciones disponen de la actualización automática y se hace efectiva cuando dispone de internet.

Para el Sistema Financiero XEO y el Software Administración Documental DOCUADMIN se realiza el mantenimiento al software periódicamente o cuando se requiera, las actualizaciones se hacen según las mejoras que hagan a los aplicativos según los desarrolladores.

13. PLATAFORMA TECNOLÓGICA PARA LA OPERACIÓN Y APLICATIVOS RECIENTEMENTE ADQUIRIDOS

13.1 Software y hardware para manejo de contingencias

Se cuenta con cuarenta y dos (42) UPS en las estaciones de trabajo donde trabajan constantemente en el software financiero XEO de la Entidad, esto con el fin de proteger los computadores en caso de una ida de luz y así evitar un apagado forzoso y pérdida de información.
El Instituto cuenta con un software antivirus licenciado, con el fin de evitar perdida de información y daños en los equipos de cómputo.

13.2 Sistemas de Backup utilizados:

Se debe tener en cuenta que la entidad cuenta con un horario laboral de 7:30 a.m. a 12:30 p.m y de 1:30 p.m. a 5:00 p.m.
Al Servidor local de IDESAN se le crea un arreglo raid 5+0, con contingencia; con 4 discos duros de 1TB; almacenados efectivo 3tb +/- 40%.
Para sistema operativo: 500 GB
Para datos 1,4 TB
Para AD: 10GB

13.3 Otras características de seguridad.

a. Dos Discos Externos en donde se realizan las copias de la información financiera – SIIARE del Instituto y la información de DOCUADMIN (Gestión Documental).
b. Se realiza la copia mensual en Disco Externo de 1T, la cual se le hace entrega a la Empresa **CONTROL ONLINE**, con el fin de ser custodiada fuera de la entidad.

c. Se creó una unidad compartida con el nombre de cada equipo desde el servidor para cada estación de trabajo con el fin de que realicen la copia de los archivos más importantes. Se dio la capacitación respectiva con instructivo en marzo 08 de 2018.

13.4 Copia de Seguridad Sistema Financiero XEO

Teniendo en cuenta que el sistema de información XEO es el activo intangible más importante dentro del IDESAN, las copias de seguridad se deben realizar con una frecuencia de al menos una vez por semana, estas pueden generarse de forma automática incluso con los usuarios operando el sistema. Se deben tener en cuenta algunos pasos para poder realizar las copias de seguridad:

- ✓ Las copias se deben realizar en el equipo servidor donde se encuentran instalados los programas XEO® y la base de datos Sybase.
- ✓ El disco del servidor donde se tenga más espacio crear la carpeta COPIAS_XEO.
- ✓ Descargar el programa libre COBIAN BACKUP 11 (Gravity) del siguientelink: http://www.cobiansoft.com/cobianbackup.htm.
- ✓ Instalar el programa COBIAN BACKUP 11 y automáticamente se instalaran los componentes necesarios para el funcionamiento del programa y al final aparecerá el icono ejecutándose en la barra de tarea el cual indica que está funcionando el programa.
- ✓ Iniciar el programa COBIAN BACKUP 11 y configurar el aplicativo para que realice las copias de seguridad automáticamente.

14. PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO

REQUERIMIENTOS TECNOLÓGICOS Y OPERATIVOS

Se recomienda que el servidor y los equipos de cómputo que utilicen el Software Sistema Financiero XEO y el Software Administración Documental DOCUADMIN cumplan con los siguientes requisitos mínimos para su debido uso dentro del IDESAN:

Requerimientos Hardware y Software del Servidor

Requerimiento Hardware		
Características	**Mínimo**	**Recomendado**
Memoria	4 GB de RAM	4 GB de RAM o superior
Disco Duro	1 TB	4 TB o superior

Procesador	Intel XeonQuadCore 4 núcleos (2 físicos y 2 lógicos)	Intel Xeon 8 núcleos (4 físicos y 4 lógicos)
Tarjeta de Red	100 Mbits	1000 Mbits
Requerimiento Software		
Características	**Mínimo**	**Recomendado**
Sistema Operativo	Windows Server Estándar 2008	Windows Server 2008 o superior.
Sistemas de Archivos	NTFS o ext3 con Samba	NTFS o ext3 con Samba

Requerimiento Hardware y Software Usuario

Requerimiento Hardware		
Características	**Mínimo**	**Recomendado**
Memoria	4 GB de RAM	4 GB de RAM o superior
Disco Duro	250 GB	250 GB o superior
Procesador	Intel Core i3 3.3 Ghz.	Intel Core i3, i5, i7
Tarjeta de Red	100 Mbits	1000 Mbits
Requerimiento Software		
Características	**Mínimo**	**Recomendado**
Sistema Operativo	Windows XP	Windows 7o Superior
Navegador de Internet	Microsoft Internet Explorer 6.0 o Chrome	Microsoft Internet Explorer 7.0 o Chrome o superior
Antivirus actualizado y licenciado.		

Aplicativos Básicos para su funcionamiento

Sistema Financiero XEO				
	Nombre	**Versión**	**Debe Licenciar**	**Características**
Lenguaje de Desarrollo	PowerBuilder	8.0	No Aplica	Cliente— Servidor
Base de Datos	Sybase SQL Anywhere y SQL Server 64 bits 2014.	10.0 o Superior	Aplica	Multiusuario
		11.0.1 Web Edition(Express versión)	No aplica (libre)	Multiusuario para 1 servidor y 3 maquinas
Software Administración Documental DOCUADMIN				

	Mínimo	**Recomendado**	**Características**

Motor Base de Datos	PostgreSQL 8.1	PostgreSQL 8.2 o Superior	Servidor
Controlador ODBC	Controlador ODBC para PostgreSQL8.0	Controlador ODBC para PostgreSQL 8.0.1 o superior	Cliente

14.1 GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

14.1.1 PLAN DE CONTINGENCIA INFORMATICO DEL INSTITUTO FINANCIERO PARA EL DESARROLLO DE SANTANDER - IDESAN

14.1.1.1 INTRODUCCIÓN

Para la realización de un plan de contingencia dentro del instituto financiero para el desarrollo de Santander – IDESAN se analiza las amenazas a la información ante la posible pérdida, destrucción y robo expuestos a diversos factores de riesgo Humanos y Físicos, a raíz de amenazas de origen natural (terremotos, tormentas, etc.), de origen humano (problemas laborales, falta de conocimiento, mala comunicación, etc.), de origen técnico (fallas de software, fallas de hardware, fallas eléctricas, etc.) y en de caso situaciones no previstas que producen daños físicos irreparables. En este documento se pretende definir las políticas de seguridad más confiables en materia de recuperación y rápido control de la información para garantizar la normalidad laboral ante la presencia de cualquier eventualidad.

Existe un Mapa de Riesgos vigencia 2013 para el Instituto Financiero para el Desarrollo de Santander, que sirve como documento base para el desarrollo del Plan de Contingencia Informático indicando los controles de seguridad física y de ambiente en manejo de la información.

14.1.1.2 OBJETIVOS

Proporcionar al Área de Sistemas del Instituto Financiero para el Desarrollo de Santander – IDESAN, una herramienta para garantizar el funcionamiento de los sistemas de información y la inmediata recuperación en el menor tiempo posible de cualquier falla de interrupción producido por corte de servicios, fenómenos naturales o humanos.

14.1.1.3 IDENTIFICACION DE RIESGOS

Principales servicios que deben ser restablecidos o recuperados por cualquier falla de interrupción.

Equipo de Computo

- Sistema Operativo.
- Correo Electrónico.
- Internet.
- Antivirus.
- Paquete Ofimático.

Software o Base de Datos

- Sistema Financiero XEO.
- Software Administración Documental DOCUADMIN.
- Ejecutables de las aplicaciones.

Copias de Seguridad

- Backup del Servidor.
- Backup del Sistema Financiero XEO.
- Backup del Software Administración Documental DOCUADMIN.
- Backup de la Información de los equipos de Computo.

14.1.2 ANALISIS DE EVALUACION DE RIESGOS Y ESTRATEGIAS

14.1.2.1 Metodología aplicada:

Se identifica un conjunto ordenado y flexible de factores que pueden dar origen a incumplimientos, o deficiencias críticas y se califica la presencia del riesgo y se prevén sus posibles daños.

El enfoque del riesgo es PREVENTIVO, mediante su identificación es posible evitar la exposición al mismo y la presencia de los efectos indeseables que generan no conformidades. Una entidad es vulnerable a riegos, cuando los factores que lo configuran están presentes, su probabilidad de ocurrencia es alta y el daño que se puede causar con su presencia es elevado.

- **Impacto:** El impacto de un evento puede ser leve, moderado o catastrófico.
- **Riesgo:** Es la vulnerabilidad de un Activo o bien, ante un posible daño potencial (Aceptable/tolerable, importante, moderado e inaceptable).
- **Tipo del Riesgo:** Existen diferentes tipos de riesgos especificados de la siguiente manera:

  Riesgos del Entorno
  - ***Riesgos Naturales:*** Tales como mal tiempo, terremotos, etc.
  - ***Riesgos Sociales:*** como actos terroristas y desordenes.

Riesgos Generados en la empresa

- **Riesgos Estratégicos:** se basa en la administración de la organización, en sus políticas, diseño de estrategias y cumplimiento de metas.
- **Riesgos Operativos:** sé relaciona con las deficiencias de la infraestructura y organización, en cuanto a las dependencias, fallas de los sistemas de información, falta de documentación de los procesos, etc.
- **Riesgos Financieros:** Es la relación del manejo eficiente y transparente de los recursos financieros del instituto.
- **Riesgos de cumplimiento:** Capacidad para el cumplimiento de los requisitos legales, Contractuales y el buen reconocimiento del instituto.
- **Riesgos Tecnológicos:** se asocia a seguridad de la tecnología disponible en la adaptación de necesidades actuales y futuras.

Al realizar un análisis de los elementos de riesgo en los cuales está expuesto los sistemas de información y los equipos de cómputo del Instituto Financiero para el Desarrollo de Santander - IDESAN, se realiza una descripción de los activos susceptibles a daño:

- ✓ Personal
- ✓ Hardware
- ✓ Software o Base de Datos
- ✓ Documentación
- ✓ Suministro de energía eléctrica
- ✓ Suministro de telecomunicaciones

14.1.4.2 Posibles Daños

- ✓ El difícil acceso a la infraestructura y recursos debido a problemas físicos en las instalaciones, por causas naturales o humanas.

- ✓ El acceso denegado a los recursos informáticos, sean por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información o procesos no deseados.
- ✓ La mala administración de la información fuera de la institución y que afecte el patrimonio estratégico, mediante Robo o Infidencia.

14.1.4.3 Fuentes de daño

- ✓ El acceso no autorizado a las instalaciones del Instituto.
- ✓ El indebido uso de las claves de acceso a los sistemas de información.
- ✓ Fenómenos Naturales (Movimientos telúricos, Inundaciones, Fallas en los equipos principales causadas por el ambiente, la red eléctrica, etc.)
- ✓ Fallas de los funcionarios (Enfermedad, Accidentes, Renuncias, Abandono de sus puestos de trabajo, etc.).

- ✓ Fallas de Hardware (Falla en los Servidores, en los equipos de cómputo, falla de Red o Switch, cableado estructurado, Router, FireWall, etc.).

14.1.4.4. Clases de Riesgos dentro del Instituto

- ✓ Ausencia de archivos Magnéticos (Backup) fuera de la entidad.
- ✓ Ausencia de Software y Hardware, como soporte tecnológico
- ✓ Deficiencia en el Sistema de Información Financiera XEO
- ✓ Pérdida de tiempo y recursos debidas a Virus electrónicos y/o a daños de equipos principales y/o auxiliares
- ✓ Intromisión, hackeo y/o robo de información neurálgica de la organización, claves electrónicas, saldos, cuentas movimientos etc. Delitos Informáticos desde los equipos y/o en contra del Instituto.
- ✓ Daños en Redes, perdida de comunicación y/o conexión entre equipos
- ✓ Uso de Software Pirata o Ilegal
- ✓ Incendio o fuego dentro de las instalaciones del instituto.
- ✓ Fenómenos Naturales (Movimientos telúricos, Inundaciones, Fallas en los equipos principales causadas por el ambiente, la red eléctrica, etc.).
- ✓ Ausencia de personal en el área de sistemas.

14.1.3 DISMINUCION DEL RIESGO

RIESGO 1: R012-01	
Ausencia de Software y Hardware, como soporte tecnológico	
Tipo de Impacto: Cuantitativo	**Tipo de evento:** Fallas Tecnológicas

Efecto	Causas	Control
La ausencia de Hardware implicaría no contar con equipos de cómputo, impresoras, etc, no se podría cumplir con el desarrollo laboral de los funcionarios, y por ende con los objetivos, misión y visión del Instituto. Con ausencia de Software el Instituto no podría llevar nada sistematizado, todo sería manual, hace lentos los procesos, duplicidad de procesos e información y no se contaría con información veraz, confiable y segura.	Perdida de la información en caso de siniestro	Se cuenta con equipos de cómputo de tecnología de punta, servidor actualizado con discos espejo
RIESGO 2: R012-02		
Alteraciones en la información suministrada por el Software Financiero de la Entidad		
Tipo de Impacto: Cuantitativo	**Tipo de evento:** Fallas Tecnológicas	
Efecto	**Causa**	**Control**
Deficiente prestación del servicio, Incumplimiento en la rendición de informes. Pérdida de Tiempo e Información no confiable.	Al ponerse a puesta y marcha el Sistema Financiero no hubo suficiente control, no se revisaron los programas adecuados y los informes que generaba el sistema.	Cada usuario cuenta con su clave y contraseña y con sus permisos.
RIESGO 3: R012-03		
Virus electrónicos y/o a daños de equipos principales y/o auxiliare.		
Tipo de Impacto: Cuantitativo	**Tipo de evento:** Fallas Tecnológicas	
Efecto	**Causa**	**Control**
Pérdida de tiempo, Incumplimiento de labores.	Infección de virus debido al acceso indebido a internet, uso de memorias USB.	Software Antivirus.

RIESGO 4: R012-04		
Intromisión, hackeo y / o robo de información neurálgica de la organización, claves electrónicas.		
Tipo de Impacto: Cualitativo	**Tipo de evento:** Fraude externo	
Efecto	**Causa**	**Control**
Perdida de información, Ilícitos Informáticos, Acceso a información clasificada.	Bajo seguridad de acceso a las oficinas y equipos de cómputo. No contar con claves de seguridad tanto en el equipo como en el software. Delitos Informáticos desde los equipos y/o en contra de la entidad.	La Institución cuenta con FIREWALL (seguridad perimetral de la información).
RIESGO 5: R012-05		
Daños en Redes, pérdida de comunicación y/o conexión entre equipos.		
Tipo de Impacto: Cualitativo	**Tipo de evento:** Fallas Tecnológicas	
Efecto	**Causa**	**Control**
Al estar trabajando en los sistemas se vuelve lento, se bloquean los procesos de cierre, generación de informes, pérdida de tiempo y de información e Incumplimiento de labores.	Subidas de voltaje, vida útil de la red o daño en la red.	La Institución cuenta con un cableado de Categoría 7a de última tecnología.
RIESGO 6: E012-06		
No se tendría acceso a la información financiera del instituto y no se podría dar atención al cliente en cuanto a pagos, estados de consulta etc.		
Tipo de Impacto: Cuantitativo	**Tipo de evento:** Daños a los Activos	
Efecto	**Causa**	**Control**

No se tendría acceso a la información financiera del instituto y no se podríadar atención al cliente en cuanto a pagos, estados de consulta etc.	Que se dañen los discos duros o daños en el procesador, etc, que nose pueda entrar al Instituto por un incendio, terremoto, etc. Y que se dañe la parte eléctrica.	La Institución debe contar con un plan de contingencia del negocio, teniendo acceso al Datacenter.

RIESGO 7: R012-07		
Desinformación a las partes interesadas a causa de la página WEB institucional desactualizada.		
Tipo de Impacto: Cuantitativo	**Tipo de evento:** Ejecución y Administración de procesos	
Efecto	**Causa**	**Control**
No se tiene establecido un listado de identificación de la información que se debe publicar, su periodicidad y los responsables del reporte y seguimiento.	Información desactualizada en la página web del instituto.	Cada funcionario es responsable de enviar la información de su área que debe estar en la página web.

14.1.4 EVENTOS CONSIDERADOS PARA EL PLAN DE CONTINGENCIA

Cuando se genera un riesgo dentro del IDESAN, este puede producir un Evento, se hace una descripción de los eventos a considerar dentro del Plan de Contingencia.

RIESGO	EVENTO
• Fallas en el Cable UTP. • Fallas en la Tarjeta de Red. • Fallas en la configuración de la dirección IP. • Fallas en el Switch. • Fallas en el Punto de Red.	No existe comunicación entre el cliente y el servidor

• Fallas en el Servidor por Hardware • Falla del UPS (Falta de Suministro eléctrico). • Virus electrónico. • Falla en el Disco por sobrepasar el límite de almacenamiento. • Colocar el servidor como un Computador de Escritorio.	Fallas en el Servidor
• Incapacidad laboral • Accidente • Renuncia Intempestiva	Ausencia de personal en el Área de Sistemas

• Fallas o corte en el Fluido Eléctrico	Interrupción del fluido eléctrico durante la ejecución de los procesos.
• Falla de equipos de comunicación: Switch o Cableado estructurado • Fallas en el software de Acceso a Internet. • Perdida de comunicación con proveedores de Internet.	Perdida de servicio de internet
• Incendio • Sabotaje • Corto Circuito • Terremoto	Perdida del centro de computo

14.1.5 DESCRIPCION DE LOS EVENTOS:

14.1.5.1 No existe comunicación entre el cliente y el servidor

a. Impacto

- ✓ Los funcionarios no pueden trabajar con los recursos de la red. Manejo de información.
- ✓ Interrupción de sus labores.

b. Procedimiento a seguir

- ✓ Solicitud que hace el usuario, porque no cuenta con acceso a la red.
- ✓ El personal encargado del área de sistemas procederá a identificar el problema.
- ✓ Si en caso de que no se resuelve el problema se procede a constatar si existe problema en la tarjeta de red, si es afirmativo se debe realizar cambio o arreglo de dicho hardware.
- ✓ Si persiste el problema revisar las conexiones de los puntos de red.
- ✓ Testear el cable UTP. Si existe daño, realizar el cambio del cable.
- ✓ Realizar el mantenimiento del punto de red lógico del usuario y del rack.
- ✓ Recuperación del sistema de red para el usuario.

c. Recursos de Contingencia

Como contingencia se utiliza el remplazo de algunos componentes:

- ✓ Tarjeta de Red
- ✓ Conector RJ-45
- ✓ Jack RJ-45
- ✓ Herramientas de Cableado Estructurado
- ✓ Conexión con el modem o switch, etc.

14.1.5.2 Fallas en el Servidor

a. Impacto

- ✓ Paralización de procesos o aplicativos que se encuentran en el servidor ya que presenta fallas.
- ✓ Posible pérdida del hardware y el software.
- ✓ Perdida de las copias de seguridad o backup del servidor.

b. Causas de la falla de Servidor

Causa 1: Error Físico del Disco

En caso dado que el disco presenta fallas que no se puedan reparar, se debe tomar las siguientes acciones:

- ✓ Encontrar el disco que presenta la falla.
- ✓ Informar a los usuarios por correo electrónico o por vía telefónica que deben salir del sistema.
- ✓ Bloquear el acceso al sistema para que el usuario no ingrese al equipo de cómputo sin autorización.
- ✓ Apagar el equipo.
- ✓ Extraer el disco dañado y reemplazarlo con otro del mismo tipo, formatearlo y darle partición.
- ✓ De forma inmediata se debe restaurar el último backup en el disco y restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
- ✓ Verificar que los sistemas que se encuentran en dicho disco estén en buen estado.
- ✓ Habilitar el acceso al sistema para los usuarios.

Causa 2: Error de Memoria RAM

- ✓ El servidor no responde correctamente debido a la lentitud de procesos o por el ingreso masivo de usuarios al sistema.
- ✓ Si existe muchos procesos al mismo tiempo puede ser que algunos otros se congelen.
- ✓ La memoria podría no estar asentada correctamente en el socket y esto puede ocasionar lentitud en los procesos.

Causa 3: Virus Electrónico

Existe la posibilidad de que se presente virus en los equipos de cómputo o en el servidor principal, se debe realizar lo siguiente:

- ✓ Se debe contar con un antivirus en el sistema que bloquee el virus que ingresa al servidor o al equipo de cómputo.
- ✓ El antivirus muestra el registro de amenazas con fecha, gravedad del virus y su ubicación dentro de los equipos de cómputo.
- ✓ En caso de que existan archivos (.exe, .com, etc.) serán reemplazados o se realizara una restauración de los Backup.
- ✓ Si los archivos infectados por el virus son bloqueados por el antivirus y sigue con el mensaje de alerta diciendo que existe virus en el sistema, lo más factible es que uno de los equipos de cómputo o servidor fue el que causó la infección, se debe restringir el ingreso al sistema y realizar su revisión.

c. Recursos de Contingencia

- ✓ Un buen aplicativo de Antivirus totalmente licenciado e instalado en el servidor.
- ✓ Componente de Remplazo si existe daño el algunas unidades (Memoria, Disco Duro, etc.)
- ✓ Backup diario de información del servidor

14.1.5.3 Ausencia de personal en el Área de Sistemas

a. Impacto

- ✓ Interrupción de funciones y procesos internos o externos del IDESAN por parte de la persona ausente
- ✓ Falta de control en la Administración de las Bases de Datos y monitoreo del servidor.
- ✓ Soporte técnico a los funcionarios.
- ✓ Falta de ajustes a los aplicativos o programas críticos del sistema.

b. Procedimiento a Seguir

- ✓ Resolución del Gerente del IDESAN indicando el funcionario encargado en las labores del área de sistemas especificando el periodo de asignación y las labores a realizar.
- ✓ Realizar un informe detallado del área de Sistemas especificando la cantidad de usuarios dentro de los sistemas y equipos de cómputo conectados en el servidor.
- ✓ Identificar la ubicación de los Backup realizados por el servidor.

c. Recursos de Contingencia

- ✓ Manual de funciones actualizado de las Bases de Datos existentes dentro del IDESAN.
- ✓ Instructivos actualizados del control de copias de seguridad, actualización del antivirus y mantenimiento interno y externo de los equipos de cómputo.
- ✓ Informes detallados de los Sistemas de Información del IDESAN.

14.1.5.4 Interrupción del fluido eléctrico durante la ejecución de los procesos

a. Impacto

- ✓ Interrupción de labores debido a las fallas eléctricas.

b. Procedimiento a seguir

- ✓ En caso de corto circuito, la UPS mantendrá encendido el servidor y los equipos de cómputo por cierto tiempo, mientras se soluciona la falla eléctrica.
- ✓ En el caso de interrupción del servicio eléctrico la UPS brinda (corriente de emergencia), hasta que los funcionarios realicen sus procesos, para que no corten bruscamente las actividades que estén realizando.

c. Recursos de contingencia

- ✓ El Área de Sistemas debe asegurarse que las UPS, se encuentren siempre cargadas.

14.1.5.5 Perdida de servicio de internet

a. Impacto

- ✓ Paralización de procesos en línea o aplicativos que se lleven a cabo por la internet.

b. Proceso a seguir

- ✓ Revisar conexiones (modem, switch, etc) para identificar las interrupciones del servicio.
- ✓ Si se identifica el problema en el hardware, se procederá a cambiar el componente.
- ✓ Si se identifica el problema con el software, se debe restaurar el sistema operativo del servidor o equipo de cómputo.
- ✓ Si no se encuentra la falla en el servidor y los equipos de cómputo, de forma inmediata llamar a la Empresa prestadora del servicio, para la asistencia técnica.
- ✓ Realizar el formato de Solicitudes y soluciones de Sistemas para llevar un control de lo realizado.
- ✓ Realizar pruebas de funcionalidad del servicio y verificar que este habilitado.

c. Recursos de Contingencia

- ✓ Revisar el Hardware y Software del servidor y equipos de cómputo.
- ✓ Revisar el Modem, Router, etc.
- ✓ Verificar que las Herramientas de Internet se encuentren activas.

14.1.5.6 Perdida del centro de cómputo

a. Impacto

- ✓ Caída de la red: Servidores y equipos de comunicación.
- ✓ Paralización de los sistemas de información y procesos que soportan las funciones del IDESAN.
- ✓ Perdida de hardware y software.

b. Proceso a seguir

- ✓ Verificar el inventario existente del área de sistemas.
- ✓ Realizar una inspección de los recursos tanto de hardware y software que se puedan salvar.
- ✓ Salvaguardar los Backup de información realizados en el servidor.
- ✓ Analizar un nuevo sitio donde se pueda restaurar el Centro de Cómputo.
- ✓ Se requiere de un presupuesto y recursos para la adquisición de un nuevo software, hardware, materiales, personal y transporte.
- ✓ Comenzar con las nuevas adecuación y configuración del centro de cómputo.
- ✓ Restaurar los Backup efectuados por el área de sistemas.

c. Recursos de Contingencia

- ✓ Es necesario que el hardware y software deba adquirirse, así como ser transportados al sitio alterno; se analizan ciertas estrategias básicas para disponer de nuevos equipos de cómputo para su reemplazo:

  - Se establecen acuerdos de nivel de servicios con los proveedores o contratista del software, hardware y medios de soporte; donde se debe especificar el tiempo de respuesta requerido.
  - Se requiere de un inventario de equipos nuevos comprados por adelantado y se almacenan en un sitio externo o sitio alterno del IDESAN.

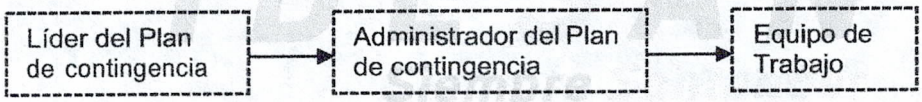
- ✓ Una manera de recuperación rápida es almacenar un equipo sin usar para comenzar rápidamente dicho proceso.
- ✓ Existe la posibilidad de un desastre extendido donde se requiere sustituir masivamente de equipos y retrasos del transporte.
- ✓ Realizar informes detallados sobre las necesidades de los equipos de cómputo y especificaciones técnicas dentro del plan de contingencia.

d. Recursos de Contingencia Generales

- ✓ Router suministrado por el proveedor de Internet.
- ✓ Servidor y Equipos de Comunicación (Switch, cable utp, etc.).
- ✓ Rack de Comunicaciones y Servidores.
- ✓ Insumos y herramientas para el cableado estructurado.
- ✓ UPS y Equipos de aire acondicionado.
- ✓ Backup de los Sistemas de información.
- ✓ Instaladores de los aplicativos: Software Base, Sistema Operativo, Utilitarios, etc.

15. PLAN DE RECUPERACIÓN Y RESPALDO DE LA INFORMACION

Para dar cumplimiento al desarrollo del plan de contingencias del área de sistemas del IDESAN, se requiere de la ejecución y estructuración de actividades para la creación de grupos encargados del desarrollo, implantación y mantenimiento de dicho plan, que facilite el normal funcionamiento de los procesos internos y externos del instituto.



ORGANIZACIÓN: Se define las responsabilidades de cada uno de los participantes de cada área.

Líder del Plan de Contingencia: Gerente

Administrador del Plan de Contingencia: Técnico de Sistemas

Equipo de Trabajo:
Oficina del Área de Sistemas.
Oficina de Planeación y Calidad
Oficina de Control Interno

15.1 RESPONSABLES

a. Líder del plan de contingencia

- ✓ Dirigir y llevar a cabo las acciones correctivas especificadas anteriormente, con el fin de disminuir los riesgos establecidos.

b. Administrador del Plan de Contingencia

- ✓ Establecer el plan de trabajo.
- ✓ Determinar los responsables y prioridades para el desarrollo de las tareas asignadas en dicho plan.
- ✓ Orientar al equipo de trabajo en la organización del proyecto.
- ✓ Establecer coordinaciones entre el Equipo de trabajo, el Líder y las demás Áreas involucradas.
- ✓ Verificar y formalizar que el proyecto sea documentado formalmente y de fácil entendimiento.
- ✓ Vigilar el desarrollo del proyecto.
- ✓ Comunicar al Líder del Proyecto, los avances y ocurrencias durante el cumplimiento de las tareas de los responsables.

c. Equipo de Trabajo

- ✓ Notificar oportunamente al Administrador del Proyecto, sobre los avances de las tareas asignadas, así como las dificultades encontradas y la identificación de los riesgos.
- ✓ Identificar aspectos operativos no contemplados en el Cronograma de actividades.
- ✓ Realizar las acciones correctivas del caso, coordinando su implementación con el Administrador del Proyecto.

El plan de recuperación se clasifica de la siguiente manera:

- Plan de Mitigación (Previas al Desastre)
- Plan de Emergencia (Durante el Desastre)
- Plan de recuperación (Después del Desastre)

15.2 Plan de Mitigación (Previas al Desastre)

Consiste en el desarrollo de estrategias y procedimientos previos a la posible materialización del riesgo u ocurrencia de la emergencia, tendientes a la mitigación de los mismos, haciéndolos menos graves, reduciendo al máximo las consecuencias o posibles pérdidas.

Se establecen los siguientes procesos:

- Sistemas de Información
- Equipos de computo
- Copias de Seguridad (Backup)

15.3 Sistemas de Información:

El Instituto deberá tener una relación de los Sistemas de Información que manejan tanto en procesos internos como externos, en caso de falta o falla de los equipos de cómputo.

Este proceso incluye componentes importantes como:

- ✓ El manejo de los Datos.
- ✓ La documentación manejada
- ✓ Las Base de datos (Sistema de Información XEO y DOCUADMIN)
- ✓ Los equipos de Computo

Para las Bases de Datos es importante la utilización de los manuales donde indique como restaurar el sistema de información en caso de daño en el equipo o software.

15.3.1 Equipos de Cómputo:

Se debe tener en cuenta que, en caso de un desastre de Hardware de los equipos de cómputo, impresoras, scanner, módems, fax entre otros, especificando su ubicación en cuanto al software que usa y al nivel de uso institucional. Se debe utilizar los siguientes criterios de identificación y protección de equipos:

- ✓ Pólizas de seguros, como parte a la protección de los activos institucionales y estableciendo una restitución de equipos, teniendo en cuenta la depreciación tecnológica.

- ✓ Identificar los equipos de cómputo de gran importancia según los procesos manejados internamente y el valor de sus componentes, para dar prioridad en caso de evacuación. Por ejemplo, etiquetar de color rojo los servidores, color amarillo a los equipos de cómputo con información importante o estratégica, y color verde a las demás estaciones (normales, sin disco duro o sin uso).

- ✓ Mantener actualizado el inventario de los equipos de cómputo, asignándole a cada equipo un respectivo número para una mejor identificación.

15.3.2 Copias de Seguridad (Backup)

Se debe contar con los medios para la obtención de las copias de seguridad de los aplicativos trabajados dentro del Instituto, que sean necesarios para asegurar la correcta ejecución de los procesos internos y externos para un mejor rendimiento de los funcionarios.

Estos Backup deben ser ejecutados de dos maneras:

- Por el administrador del Área de Sistemas
- Por los usuarios con privilegios para realizar copias de seguridad.

Las copias de seguridad se realizan con el Instructivo 32.027.004-002 llamado Control de Copias de Seguridad.

Existen dos formas de realizar las copias de seguridad dentro del IDESAN:

1. **Copia de Seguridad en el servidor:** Se creó una unidad compartida con el nombre de cada equipo desde el servidor para cada estación de trabajo, con el fin de que realicen la copia de los archivos más importantes.

    - Oficina de Sistemas: TODOS LOS DÍAS se realiza copia de seguridad en el servidor.
    - CONTROL ONLINE: UNA COPIA MENSUAL se realiza en un disco duro 1T, la cual se le hace entrega a la empresa CONTROL ONLINE. con el fin de ser custodiada la información fuera de la entidad.

15.4 Plan de Emergencia (Durante el Desastre)

En esta etapa incluye las acciones detalladas de las actividades que se deben realizar durante la emergencia, si esto ocurre en el día, en la noche o en la madrugada. Suministrar instrucciones en las áreas operativas y administrativas, en caso de materializarse el riesgo.

Tener en cuenta que soluciones deben ser implementadas para conservar los procesos críticos en el momento de la materialización de los riesgos, para cada proceso crítico asociado a un riesgo, se define una acción o procedimiento a seguir.

15.4.1 Software

En esta etapa se incluye los procesos o aplicativos que llegan a un estado crítico en el momento de materializarse el riesgo, como son:

15.4.1.1 Sistemas Financiero XEO

Aplicación XEO: Módulos de Contabilidad- Activos Fijos, Presupuesto, Nomina, Cartera Financiera y Ahorros, Central de riesgos de Cartera – Cifín, Descuentos por Libranza, Convenios, Gerencial de Contabilidad y Control de cartera financiera de terceros, colocaciones especiales, el GAP de liquidez y el módulo de la DIAN

Estado Actual: Se contrató con el proveedor para el Mantenimiento preventivo, correctivo y revisión permanente al software XEO y Software SIIARE donde la empresa ofrece al Instituto configuración, consultoría, soporte correctivo, evolutivo, actualizaciones, y capacitación al personal en el manejo de los aplicativos, mantenimiento y revisión del Aplicativo Xeo Gestión Oficial: Contabilidad Oficial, Activos Fijos, Presupuesto Oficial, Cartera Financiera y ahorros, Central Riesgo de Cartera – Cifin, Descuentos por Libranza, Convenios, Gerencial de Contabilidad, Riesgo de Liquidez – Formato 458, información exógena DIAN formatos 1001, 1003, 1007, 1008, 1009, 1010, 1011 y 1012, NIIF, Informes Superfinanciera formatos 509, 510, 511, 512, 513, 514 y 515, Flujo de trabajo en fábrica de crédito, Pago y aplicación de abonos en línea mediante botón de pagos y servicio de mantenimiento para el software Web SIIARE de administración del riesgo empresarial: SARO, SARLAFT, SARC, SARM y SARL. Con esta empresa se adquirió la licencia de uso por tiempo ilimitado del software ya que son los únicos desarrolladores del Software Financiero XEO.; para su buen y correcto funcionamiento.

Proveedores: TECNOINFORMATICA.S.A.S

Usuario: Financiera, Convenios; Contabilidad, Planeación, Cartera, Tesorería, Asesor Comercial, Riesgos, Control Interno y Sistemas.

Riesgos Asociados: incumplimiento del contratista con el objeto contractual, Existe la posibilidad de retrasos en los Procesos Administrativos, Mal funcionamiento del aplicativo o del equipo de cómputo donde esté instalado el software.

Soluciones en contingencia: Ante la posible materialización de los riesgos o falla del aplicativo se plantea las siguientes soluciones:

1) Restaurar las copias de seguridad: Las copias se deben realizar en el equipo servidor donde se encuentran instalados los programas XEO® y la base de datos Sybase. Dichas copias de seguridad son realizadas con el aplicativo COBIAN BACKUP 11.

2) El contratista va a tener acceso a las copias de seguridad efectuadas con anterioridad, y el desarrollador del aplicativo envía las actualizaciones realizadas a la Base de Datos para ser instaladas nuevamente en el servidor.

3) Teniendo la Base de datos Actualizada se da la opción de volver a Subir el Software al servidor, se le informa a los usuarios que pueden empezar a trabajar con el aplicativo.

15.4.1.2 Software Administración Documental - DOCUADMIN

Aplicación DOCUADMIN: Trabaja en el Módulo de Archivo: organiza documentos digitales en una base de datos de una manera jerárquica y organizada, lo cual facilita la exploración y visualización de los mismos.

Proveedores: NUMERICA LTDA

Usuario: Planeación y Archivo.

Riesgos Asociados: incumplimiento del contratista con el objeto contractual, Existe la posibilidad de retrasos en los Procesos Administrativos, Mal funcionamiento del aplicativo o del equipo de cómputo donde esté instalado el software.

Soluciones en contingencia: Ante la posible materialización de los riesgos o falla del aplicativo se plantea la siguiente solución:

1) Restaurar las copias de seguridad realizadas en el servidor e instalar las últimas actualizaciones del aplicativo.

15.4.1.3 Software Ofimático

Estado Actual: El Instituto actualmente cuenta con el siguiente software:

Software Ofimático: Microsoft Office 2003, Microsoft Office PYME y Professional 2007, Microsoft Office Hogar y pequeña empresa 2010.

Software Operativo: Windows XP, Windows Vista, Windows Server 2008 y Windows 7.

Proveedores: Distribuidores autorizados por Microsoft

Usuario: Todas las dependencias.

Riesgos Asociados: Mal funcionamiento del aplicativo o del equipo de cómputo donde esté instalado el software, Posible pérdida de información, Posible falla de equipos electrónicos y Hardware fuera de inventario.

Soluciones en contingencia: Ante la posible materialización de los riesgos, se implementa la utilización de los medios originales del software licenciado existente para reinstalar la aplicación.

15.4.2 Hardware

15.4.2.1 Servidor y Equipos de Computo

Estado Actual: Actualmente están en funcionamiento 1 servidor, 37 computadores y 14 portátiles distribuidos en las diferentes dependencias del Instituto.

Se contrató con el proveedor para el Mantenimiento preventivo y correctivo al equipo de cómputo, servidor e impresoras.

Usuario: Todos los funcionarios que necesiten un equipo de cómputo.

Riesgos Asociados: Incumplimiento del contratista con el objeto contractual, Existe la posibilidad de retrasos en los Procesos Administrativos, Mal funcionamiento del aplicativo o del equipo de cómputo donde esté instalado el software. Posible pérdida de información, Contratación o aplicación de Soluciones Inadecuadas o Incompatibles con los Recursos Disponibles, Posible falla de equipos electrónicos y Hardware fuera de inventario.

Soluciones en contingencia: Se debe garantizar el mantenimiento preventivo y correctivo de todos los equipos de cómputo y servidor diligenciando el formato de Hoja de vida y la renovación de algunos equipos de cómputo por equipos de última tecnología.

15.4.2.2 Equipos Electrónicos

Estado Actual: Se cuenta con 42 UPS en todas las dependencias.

Se contrató con el proveedor para el Mantenimiento preventivo y correctivo al equipo de cómputo, servidor, impresoras y UPS.

Usuario: Todas las dependencias del Instituto

Riesgos Asociados: Posibles retrasos en procesos administrativos, demoras en la efectividad de algunas comunicaciones, problemas en el control de asistencia del personal, Posible daño de equipos o pérdida de protección ante ausencia de fuente regulada y soporte en corte de energía eléctrica.

Soluciones en contingencia: Se debe garantizar el mantenimiento preventivo y correctivo de todos los equipos de cómputo, servidor y UPS diligenciando el formato de Hoja de vida. En el caso de no contar con fluido eléctrico regulado los equipos deben estar protegidos con reguladores de voltaje.

15.5 Plan de recuperación (Después del Desastre)

Después de ocurrido el siniestro se deben realizar ciertas actividades, tales como:

a. Evaluación de daños

Analizar y evaluar la magnitud del daño producido, es decir, que sistemas de información se están afectando, que equipos de cómputo han quedado en mal estado, cuales se pueden recuperar y en cuanto tiempo. La recuperación y puesta en marcha del servidor donde aloja dichos sistemas de información.

b. Priorizar Actividades

La evaluación de los daños reales dará una lista de las actividades que se deben realizar, de las estratégicas a implementar para el Instituto. Dichas actividades abarcan la recuperación y puesta en marcha del servidor, de los equipos de cómputo y los Sistemas de Información, compra de accesorios dañados, etc.

c. Ejecución de actividades

La ejecución de dichas actividades implica la vinculación de todos los funcionarios, creando Equipos de Trabajo para asignar actividades. Cada equipo deberá contar con un líder que es la persona indicada para informar el avance de los trabajos de recuperación y en caso de producirse un problema reportarlo de manera inmediata al Directivo, brindando posibles soluciones.

Las actividades y trabajos de recuperación se iniciarán con la restauración del servicio usando los recursos del Instituto, teniendo en cuenta que en la evaluación de daños se contempló y gestiono la adquisición de accesorios dañados.

Se requiere volver a contar con los recursos de los sistemas de información y equipos de cómputo en los lugares apropiados, se debe contar con la rapidez y eficiencia para no perjudicar la operatividad del Instituto y el buen servicio de nuestro sistema e Imagen Institucional.

d. Evaluación de Resultados

Concluidas las labores de Recuperación de los sistemas de información que fueron afectados por el siniestro, se debe evaluar objetivamente, todas las actividades realizadas por los funcionarios, con que eficacia se hicieron, que tiempo tomaron, como se comportaron los equipos de trabajo, etc.

De la evaluación de resultados y del siniestro, debe obtenerse dos tipos de recomendaciones o conclusiones:

- Retroalimentación del Plan de Contingencias Informático.
- Una lista de recomendaciones o mejoras para minimizar los riesgos y pérdidas que ocasionaron el siniestro.

15.6 CONCLUSIONES

El presente Plan de contingencias Informático del Instituto Financiero para el Desarrollo de Santander – IDESAN tiene como fundamental objetivo el proteger la infraestructura y los Sistemas de Información tomando medidas de seguridad para minimizar riesgos en caso de siniestro.

El Plan de Contingencia Informático, es un instrumento de gestión para las Tecnologías de la Información y Comunicación, cuyo fin es permitir un funcionamiento continuo en algunas funciones que se viese dañada por un accidente interno o externo. Es un avance a la hora de contrarrestar cualquier eventualidad o riesgo, que puedan ocasionar importantes pérdidas y llegado el caso no solo material sino personales y de información.

Las principales actividades requeridas para la implementación del Plan de Contingencia son: Identificación de riesgos, Análisis de evaluación de Riesgos y estrategias, Disminución de Riesgos, Eventos Considerados para el Plan de Contingencia, Descripción de los Eventos, Plan de Recuperación y Respaldo de la Información, Plan de Mitigación (Previas al Desastre), Plan de Emergencia (Durante el Desastre), Plan de recuperación (Después del Desastre).

15.7 RECOMENDACIONES

- ✓ Contar con el Plan de Contingencia del Negocio en el Instituto, que la gerencia apruebe llevar a cabo dicho proceso de contratación y posteriormente proceder a:

- ✓ Realizar una reunión general informando el contenido del presente Plan de Contingencias Informático, con el objetivo de capacitar adecuadamente a los funcionarios del IDESAN.

- ✓ Adicionalmente al plan de contingencias se deben desarrollar las acciones correctivas planteadas para minimizar los riesgos identificados.

- ✓ Es de gran importante tener garantía de los contratos con los proveedores y tener las licencias tanto de hardware como de software, así como las pólizas de seguros.

- ✓ Cuando el funcionario del área de Sistemas se encuentre ausente se recomienda capacitar a una persona que pueda desempeñar las funciones mínimas para reestablecer todos los procesos y servicios, a fin de que no se interrumpan las labores básicas del Instituto.

16. MEDICIÓN: INDICADORES (TABLERO DE CONTROL)

El IDESAN cuenta con un sistema de medición y control de indicadores relacionados de la siguiente manera:

- Eficiencia solución de sistemas a los equipos de cómputo tanto de hardware como software.
- Eficacia solución necesidades al sistema financiero XEO.
- Efectividad equipos de cómputo.
- Efectividad servicio de la oficina de sistemas.
- Actualización página web instituto.
- Avance definición e implementación del plan de contingencia de negocio.
- Eficacia avance plan de mejoramiento - gestión de sistemas.

17. MONITOREO Y SEGUIMIENTO

Los indicadores son medidos trimestralmente de la siguiente manera:

FORMATO FICHA DE INDICADORES DE GESTIÓN	60.038.02-126 versión 01 30/08/2017

Nombre del indicador:	% EFICIENCIA SOLUCIÓN SISTEMAS A LOS EQUIPOS DE COMPUTO TANTO DE HARDWARE COMO SOFTWARE
Tipo de indicador:	EFICIENCIA
Proceso relacionado:	GESTIÓN DE SISTEMAS
Fórmula del indicador:	# SOLICITUDES QUE SE ATIENDEN ANTES DE 24HRAS / TOTAL SOLICITUDES ATENDIDAS x 100%
Frecuencia de medición:	TRIMESTRAL
Meta:	80%
Calificacion:	>=80% EXCELENTE 79% - 60% REGULAR < 60% DEFICIENTE
Frecuencia de analisis y evaluacion	ANUAL
Responsable:	TÉCNICO EN SISTEMAS

Trimestral	Resultado	Meta	TOTAL SOLICITUDES ATENDIDAS	# SOLICITUDES QUE SE ATIENDEN ANTES DE 24HRAS	Calificación Trimestre	Calificación Año
I Trimestre	100.00%	80%	6	6	EXCELENTE	EXCELENTE
II Trimestre	100.00%	80%	16	16	EXCELENTE	
III Trimestre	91.30%	80%	46	42	EXCELENTE	
IV Trimestre	92.31%	80%	26	24	EXCELENTE	
ACUMULADO - META	96%				EXCELENTE	

FORMATO FICHA DE INDICADORES DE GESTIÓN	60.038.02-126 versión 01 30/08/2017

Nombre del indicador:	% EFICACIA SOLUCIÓN NECESIDADES AL SISTEMA FINANCIERO XEO
Tipo de indicador:	EFICACIA
Proceso relacionado:	GESTIÓN DE SISTEMAS
Fórmula del indicador:	SOLICITUDES ATENDIDAS / TOTAL REQUERIMIENTOS x 100%
Frecuencia de medición:	MENSUAL
Meta:	80%
Calificacion:	>=80% EXCELENTE 79% - 60% REGULAR < 60% DEFICIENTE
Frecuencia de analisis y	TRIMESTRAL
Responsable:	TÉCNICO EN SISTEMAS

Trimestre	Mensual	Resultado	Meta	TOTAL REQUERIMIENTOS	SOLICITUDES ATENDIDAS	Calificación Mes	PROMEDIO TRIMESTRE	Calificación Trimestre
I Trimestre	ENERO	100.00%	80%	6	6	EXCELENTE	100.00%	EXCELENTE
	FEBRERO	100.00%	80%	8	8	EXCELENTE		
	MARZO	100.00%	80%	9	9	EXCELENTE		
II Trimestre	ABRIL	85.71%	80%	14	12	EXCELENTE	96.24%	EXCELENTE
	MAYO	100.00%	80%	14	14	EXCELENTE		
	JUNIO	100.00%	80%	8	8	EXCELENTE		
III Trimestre	JULIO	95.24%	80%	21	20	EXCELENTE	91.69%	EXCELENTE
	AGOSTO	90.91%	80%	11	10	EXCELENTE		
	SEPTIEMBRE	88.89%	80%	9	8	EXCELENTE		
IV Trimestre	OCTUBRE	88.89%	80%	9	8	EXCELENTE	96.30%	EXCELENTE
	NOVIEMBRE	100.00%	80%	3	3	EXCELENTE		
	DICIEMBRE	100.00%	80%	2	2	EXCELENTE		

FORMATO FICHA DE INDICADORES DE GESTIÓN	60.038.02-126 versión 01 30/08/2017

Nombre del indicador:	% EFECTIVIDAD EQUIPOS DE CÓMPUTO
Tipo de indicador:	EFECTIVIDAD
Proceso relacionado:	GESTIÓN DE SISTEMAS
Fórmula del indicador:	EQUIPOS CON PROMEDIO SUPERIOR A 80% / TOTAL DE EQUIPOS x 100%
Frecuencia de medición:	ANUAL
Meta:	80%
Calificacion:	>=80% EXCELENTE 79% - 60% REGULAR < 60% DEFICIENTE
Frecuencia de analisis y	ANUAL
Responsable:	TÉCNICO EN SISTEMAS

Anual	Resultado	Meta	TOTAL DE EQUIPOS	EQUIPOS CON PROMEDIO SUPERIOR A 80%	Calificación Año
Año 2.016	72.50%	80%	40	29	REGULAR
Año 2.017	87.50%	80%	40	35	EXCELENTE
Año 2.018	84.62%	80%	52	44	EXCELENTE
Año 2.019	84.62%	80%	52	44	EXCELENTE
Año 2.020	84.62%	80%	52	44	EXCELENTE
ACUMULADO - META	**80.00%**				**EXCELENTE**

FORMATO FICHA DE INDICADORES DE GESTIÓN	60.038.02-126 versión 01 30/08/2017

Nombre del indicador:	% EFECTIVIDAD SERVICIO DE LA OFICINA DE SISTEMAS
Tipo de indicador:	EFECTIVIDAD
Proceso relacionado:	GESTIÓN DE SISTEMAS
Fórmula del indicador:	Σ CALIFICACIONES APLICADAS / TOTAL ENCUESTAS APLICADAS x 100%
Frecuencia de medición:	TRIMESTRAL
Meta:	80%
Calificacion:	>=80% EXCELENTE 79% - 60% REGULAR < 60% DEFICIENTE
Frecuencia de analisis y	TRIMESTRAL
Responsable:	TÉCNICO EN SISTEMAS

Trimestral	Resultado	Meta	TOTAL ENCUESTAS APLICADAS	Σ CALIFICACIONES APLICADAS	Calificación Trimestre
I Trimestre	90.00%	80%	40	36	EXCELENTE
II Trimestre	95.29%	80%	85	81	EXCELENTE
III Trimestre	90.53%	80%	95	86	EXCELENTE
IV Trimestre	87.69%	80%	65	57	EXCELENTE
ACUMULADO - META	**91%**				**EXCELENTE**

FORMATO FICHA DE INDICADORES DE GESTIÓN	60.038.02-126 versión 01 30/08/2017

Nombre del indicador:	ACTUALIZACIÓN PÁGINA WEB INSTITUTO
Tipo de indicador:	EFECTIVIDAD
Proceso relacionado:	GESTIÓN DE SISTEMAS
Fórmula del indicador:	REQUERIMIENTOS ACTUALIZADOS ANTES DE 3 DIAS HÁBILES / REQUERIMIENTOS RECIBIDOS x 100%
Frecuencia de medición:	TRIMESTRAL
Meta:	80%
Calificacion:	>=80% EXCELENTE 79% - 60% REGULAR < 60% DEFICIENTE
Frecuencia de analisis y	TRIMESTRAL
Responsable:	TÉCNICO EN SISTEMAS

Trimestral	Resultado	Meta	REQUERIMIENTOS RECIBIDOS	REQUERIMIENTOS ACTUALIZADOS ANTES DE 3 DIAS HÁBILES	Calificación Trimestre
I Trimestre	100.00%	80%	16	16	EXCELENTE
II Trimestre	100.00%	80%	6	6	EXCELENTE
III Trimestre	100.00%	80%	9	9	EXCELENTE
IV Trimestre	100.00%	80%	14	14	EXCELENTE
ACUMULADO - META	**100%**				**EXCELENTE**

FORMATO FICHA DE INDICADORES DE GESTIÓN	60.038.02-126 versión 01 30/08/2017

Nombre del indicador:	% AVANCE DEFINICIÓN E IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA DE NEGOCIO
Tipo de indicador:	EFICIENCIA
Proceso relacionado:	GESTIÓN DE SISTEMAS
Fórmula del indicador:	ACTIVIDADES REALIZADAS / ACTIVIDADES PROGRAMADAS x 100%
Frecuencia de medición:	ANUAL
Meta:	80%
Calificacion:	>=80% EXCELENTE 79% - 60% REGULAR < 60% DEFICIENTE
Frecuencia de analisis y	ANUAL
Responsable:	TÉCNICO EN SISTEMAS

Anual	Resultado	Meta	ACTIVIDADES PROGRAMADAS	ACTIVIDADES REALIZADAS	Calificación año
2016	100.00%	80%	1	1	EXCELENTE
2017	100.00%	80%	1	1	EXCELENTE
2018	100.00%	80%	1	1	EXCELENTE
2019	#¡DIV/0!	80%	0	0	#¡DIV/0!
2020	#¡DIV/0!	80%	0	0	#¡DIV/0!
ACUMULADO - META	**#¡DIV/0!**				**#¡DIV/0!**

FORMATO FICHA DE INDICADORES DE GESTIÓN	60.038.02-126 versión 01 30/08/2017

Nombre del indicador:	% EFICACIA AVANCE PLAN DE MEJORAMIENTO - GESTIÓN DE SISTEMAS
Tipo de indicador:	EFICACIA
Proceso relacionado:	GESTIÓN DE SISTEMAS
Fórmula del indicador:	ACCIONES CUMPLIDAS / ACCIONES PLANEADAS x 100%
Frecuencia de medición:	TRIMESTRAL
Meta:	80%
Calificacion:	>=80% EXCELENTE 79% - 60% REGULAR < 60% DEFICIENTE
Frecuencia de analisis y Responsable:	TRIMESTRAL TÉCNICO EN SISTEMAS

Trimestral	Resultado	Meta	ACCIONES PLANEADAS	ACCIONES CUMPLIDAS	Calificación Trimestre
I Trimestre	69.23%	80%	13	9	REGULAR
II Trimestre	76.92%	80%	13	10	REGULAR
III Trimestre	76.92%	80%	13	10	REGULAR
IV Trimestre	78.57%	80%	14	11	REGULAR
ACUMULADO - META	**75%**				**REGULAR**

Elaboró: ***Ing Edwin O. Correa*** -Ingeniero de sistemas
Contratista Idesan 2022

Reviso: Dra. **Ana Milena Tristancho Ballesteros**
Coordinadora Grupo Financiero y Administrativo