ALCALDÍA MAYOR
DE BOGOTÁ D.C.

ACUERDO DE JUNTA DIRECTIVA No. 010 de 2018

"Por medio del cual aprueba el Manual de Seguridad de la Tecnología de la Información del FONCEP"

LA JUNTA DIRECTIVA DEL FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES – FONCEP

En uso de sus facultades legales y en especial las que le confiere el artículo 67 literal b del Acuerdo 257 de 2006 y el artículo 1º del Decreto No. 396 del 11 de noviembre de 1996 y,

CONSIDERANDO

Que de conformidad con lo dispuesto en el artículo 60 del Acuerdo 257 de noviembre 30 de 2006 expedido por el Concejo de Bogotá, D.C., El FAVIDI se trasformó en el FONCEP, establecimiento público del orden distrital, con personería jurídica, autonomía administrativa y patrimonio propio, adscrito a la Secretaría de Hacienda.

Que el artículo 65 del Acuerdo 257 del 30 de noviembre de 2006, expedido por el Concejo de Bogotá, D.C., establece que el objeto del FONCEP, es el de reconocer y pagar las cesantías y las obligaciones pensionales a cargo del Distrito Capital, el cual asume la administración del Fondo de Pensiones Públicas de Bogotá.

Que el FONCEP, tiene las siguientes funciones básicas:

a. Reconocer y pagar las cesantías de las servidoras y servidores públicos del Distrito Capital.
b. Pagar las obligaciones pensionales legales y convencionales de los organismos del Sector Central y las entidades descentralizadas a cargo del Fondo de Pensiones Públicas de Bogotá y reconocer y pagar las obligaciones pensionales que reconozca a cargo de las entidades del nivel central y las entidades descentralizadas que correspondan, de acuerdo con los mecanismos legales establecidos.

Que el Departamento Administrativo de la Función Pública DAFP emitió Guía para la Administración del Riesgo en la que se define como riesgos de Tecnología los relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión y así mismo fijo lineamientos y aclaraciones sobre la aplicación de la metodología de administración de riesgos.

Que mediante norma ISO 31000:2009 se proporcionan principios y directrices sobre la gestión del riesgo.

Que el Sistema Integrado de Gestión Distrital NTD-SIG 001:2011 define requerimientos generales de los diferentes subsistemas y su articulación con el propósito de lograr una gestión efectiva.

Que el Decreto 2573 del 12 diciembre de 2014 establece los lineamientos generales de la Estrategia de Gobierno en línea.

Que mediante Resolución DG-0231 del 11 de julio de 2016 el FONCEP adoptó la Política de Seguridad de la Información.

Que mediante la Norma Técnica Colombiana NTC-ISO-IEC 27001 se brinda un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).

Que en la Guía Técnica Colombiana GTC-ISO/IEC 27002 se fija la selección de controles dentro del proceso de implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) con base en la NTC-ISO/IEC 27001.

Que mediante la Ley 1581 de 2012 se dictan disposiciones generales para la protección de datos personales.

Que la Ley 1712 de 2014 o de Transparencia y del Derecho de Acceso a la Información Pública Nacional es la herramienta normativa que regula el ejercicio del derecho fundamental de acceso a la información pública en Colombia.

Que a través de la norma Estándar TIA-954 se establecen recomendaciones y directrices (*guidelines*) para la instalación de infraestructuras de centros de datos.

Que la información es el activo más importante de una organización y adopta diferentes formas como: impresa, escrita, papel, digital, correo electrónico, páginas web, archivos magnéticos, sistemas de información, videos o conversaciones que requiere su adecuada protección mediante la implementación de un conjunto de políticas, procesos, procedimientos, controles, hardware y software; pero lo más importante, mediante comportamientos éticos de las personas.

Que la alta dirección, como máxima autoridad dentro de la entidad, mediante la Resolución DG-0231 del 11 de julio de 2016 establece de forma clara las líneas de actuación y manifestado su apoyo y compromiso incondicional a la seguridad de la información, con el fin de garantizar su implementación en toda la organización y sus procesos, cumpliendo con las disposiciones del Ministerio de Tecnologías de la Información y las Comunicaciones adoptando el Modelo de Seguridad y Privacidad de la Información MSPI, en el marco de la Estrategia de Gobierno en Línea – GEL y en el de su transformación a Política de Gobierno Digital.

En mérito de lo expuesto, la Honorable Junta Directiva del FONCEP,

ACUERDA

CAPÍTULO I. GENERALIDADES

ARTÍCULO PRIMERO: Objeto. El Objeto del presente Acuerdo de Junta Directiva es presentar los elementos de seguridad tecnológica implementados para la protección de la información del FONCEP.

ARTÍCULO SEGUNDO: Alcance. Los lineamientos del presente manual incluyen la definición de la Política General de la Seguridad de la Información y las políticas específicas asociadas al Modelo de Seguridad y Privacidad de la Información (MSPI) establecido en la Estrategia de Gobierno en Línea – GEL, y finaliza con los elementos de seguridad tecnológica implementados para la protección de la información del FONCEP.

ARTÍCULO TERCERO: Política General de Seguridad de la Información. El FONCEP, como entidad responsable de garantizar los derechos prestacionales y de seguridad social de sus afiliados, es consciente de que la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad al interior del FONCEP.

PARÁGRAFO PRIMERO: El cumplimiento de Política General de Seguridad de la Información permite al FONCEP:

- Identificar y minimizar los riesgos a los cuales se exponen sus activos de información, preservando la confidencialidad, integridad y disponibilidad.

- Establecer una cultura de seguridad que garantice el cumplimiento de los requerimientos legales, contractuales y técnicos mediante la adopción de las mejores prácticas.

PARÁGRAFO SEGUNDO: La Política General de Seguridad de la Información de FONCEP está soportada por políticas, normas y procedimientos específicos los cuales rigen la gestión adecuada de la información.

PARÁGRAFO TERCERO: Adoptar los siguientes principios para lograr los objetivos de Seguridad de la Información

1. Todo el personal debe conocer y responder por la seguridad de la información que gestiona de acuerdo con sus funciones.
2. Se deben tomar medidas para implementar los controles de seguridad de la información que apliquen en los procesos de la Entidad.
3. Se debe promover una cultura organizacional de mejora continua orientada a la seguridad de la información.
4. Las máximas autoridades de la Entidad deben comprometerse con la difusión, consolidación y cumplimiento de las políticas de seguridad de la información.
5. Se deben mantener las políticas, normativas y procedimientos actualizados, con el fin de asegurar su vigencia y nivel de eficacia.
6. Se debe hacer seguimiento a los riesgos de seguridad de la información y tomar acciones cuando los cambios den como resultado riesgos que no sean aceptables.

7. Se deben analizar y aplicar las medidas pertinentes cuando se presenten situaciones que puedan poner a la Entidad en situación de incumplimiento frente a las políticas, procedimientos, leyes y reglamentos relacionados con la seguridad de la información.
8. Las políticas, controles implementados, al igual que la ejecución del MSPI, será revisada con regularidad como parte del proceso del mejoramiento continuo, o cuando se identifiquen cambios en la Institución, su estructura, sus objetivos o alguna condición que afecten, para asegurar que sigue siendo adecuadas y ajustadas a los requerimientos identificados.
9. Los activos de información serán identificados y clasificados para establecer los mecanismos de protección necesarios.

ARTÍCULO CUARTO: Personas Vinculadas. Todas las personas naturales y jurídicas vinculadas o que laboren en el FONCEP serán responsables por el cumplimiento de las políticas, controles, normas, procedimientos y estándares vigentes respecto a la seguridad de la información.

ARTÍCULO QUINTO: Alcance de la Política de Seguridad de la Información. Teniendo como marco la norma técnica NTC-ISO/IEC 27001 en su versión 2013, la política de seguridad de la información del FONCEP, está dirigida a:

1) Todas las personas vinculadas al FONCEP como funcionario de carrera administrativa, libre nombramiento y remoción, provisionalidad, temporalidad, contratista y pasante;

2) Todo el personal vinculado con firmas que prestan servicios al FONCEP.

3) Todos los recursos y activos de información del FONCEP.

4) Todos los procesos y procedimientos del FONCEP.

5) Toda la infraestructura tecnológica y los Sistemas de Información que soportan la funcionalidad del FONCEP.

6) Todas las sedes físicas del FONCEP.

ARTÍCULO SEXTO: Funciones de la Alta Dirección. Adoptar como responsabilidades de la Alta Dirección las siguientes:

- Liderar el compromiso con respecto al Modelo de Seguridad y Privacidad de la Información asegurando que se establezca en la Política de Seguridad de la Información y los objetivos de la seguridad de la información.
- Asegurar que los objetivos de la seguridad de la información sean compatibles con la dirección estratégica de la organización.

- Garantizar que la Seguridad de la Información se aborde adecuadamente en toda la Entidad.

ARTÍCULO SÉPTIMO: Funciones del Comité de Seguridad de la Información. El Comité de Seguridad de la Información o el que haga sus veces debe:

- Garantizar que la Seguridad de la información se aborde adecuadamente en toda la Entidad.
- Asegurar el cumplimiento del plan de implementación y sostenimiento del MSPI.

ARTÍCULO OCTAVO: Responsabilidades de funcionarios y personas vinculadas. Todos funcionarios y vinculados con el FONCEP son responsables de:

- Velar por la protección de la información que se gestiona en sus respectivas áreas, de acuerdo con las políticas y normas de Seguridad de la Información del FONCEP
- Realizar el levantamiento de los activos de información de cada una de sus áreas.

ARTÍCULO NOVENO: Líderes del proceso. Cada líder de proceso, debe:

- Garantizar que se incluyan los lineamientos dados en las políticas y normas de Seguridad de la Información en sus procesos.

ARTÍCULO DÉCIMO: Principios Básicos. La seguridad de la información es la preservación de tres principios básicos para el manejo de la información y de los sistemas implicados en su tratamiento, así:

1) **Confidencialidad.** Propiedad que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
2) **Integridad:** Propiedad de la exactitud y completitud de la información y sus métodos de proceso.
3) **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona, entidad o proceso autorizado.

ARTÍCULO DÉCIMO PRIMERO: Políticas y procedimientos asociados. El FONCEP cuenta con políticas adicionales relacionadas con actividades puntuales que determinan el comportamiento y los lineamientos en materia de seguridad de la información:

1) **Organización de la seguridad de la información**[1]: Define el marco de referencia para operar la seguridad de la información dentro de la entidad.

[1] Ver detalle de la política en el documento MOI-GSI-GSE-001 Modelo de Seguridad y Privacidad de la Información.

2) **Seguridad de los Recursos Humanos**[2]: Establece las responsabilidades del personal en materia de seguridad de la información antes, durante y después de la contratación de los funcionarios.

3) **Gestión de Activos de Información**[3]: Define las políticas generales para mantener el inventario los activos de información, así como los propietarios y responsable de los mismos.

4) **Control de acceso**[4]: Establece las políticas generales para asegurar un acceso controlado a la información y a las aplicaciones.

5) **Criptografía**[5]: Define las políticas generales para el intercambio seguro de información o su almacenamiento.

6) **Seguridad Física**[6]: Relaciona las políticas generales para prevenir el acceso no autorizado a las instalaciones de procesamiento de información.

7) **Seguridad de las Operaciones**: Garantizar la existencia de procedimientos, registros y guías de trabajo debidamente documentados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura informática.

8) **Seguridad de las Comunicaciones**: Asegurar la protección de la información en las redes locales y las conexiones con redes externas.

9) **Adquisición, desarrollo y mantenimiento de sistemas**: Garantizar que la Política de Seguridad esté incorporada a los sistemas de información.

10) **Relaciones con los proveedores**[7]: Garantizar que la relación con los proveedores este claramente definida y ajustada a las necesidades de Seguridad de la de información.

11) **Gestión de incidentes de seguridad de la información**[8]: Gestionar las incidencias que afectan a la seguridad de la Información.

12) **Aspectos de seguridad de la información de la gestión de continuidad de negocio**: Considerar la continuidad de seguridad de la información en los procesos de gestión de la continuidad de negocio de la Entidad.

---

[2] Ver detalle de la política en el documento MOI-GSI-GSE-001 Modelo de Seguridad y Privacidad de la Información.
[3] Ver detalle de la política en el documento POL-GSI-GSE001 POLÍTICA DE USO APROPIADO DE LOS ACTIVOS DE INFORMACIÓN.
[4] Ver detalle de la política en el documento POL-GSI-GSE002 POLÍTICA DE CONTROL DE ACCESO A SERVICIOS DE TI.
[5] Ver detalle de la política en los documentos POL-GSI-GSE005 POLÍTICA DE SEGURIDAD DE INTERCAMBIO DE INFORMACIÓN y POL-GSI-GSE007 POLÍTICA DE CRIPTOGRAFÍA.
[6] Ver detalle de la política en el documento POL-GSI-GSE003 POLÍTICA DE SEGURIDAD FÍSICA.
[7] Ver detalle de la política en el documento POL-GSI-GSE004 POLÍTICA DE PROVEEDORES.
[8] Ver detalle del procedimiento en el documento PDT-GSI-GST004 PROCEDIMIENTO MANEJO DE INCIDENTES.

ACUERDO DE JUNTA DIRECTIVA No. 010 de 2018
"Por medio del cual aprueba el Manual de Seguridad de la Tecnología de la Información del FONCEP"

13) **Cumplimiento**: Prevenir los incumplimientos de las leyes penales o civiles, de las obligaciones reglamentarias o contractuales y de las exigencias de seguridad.

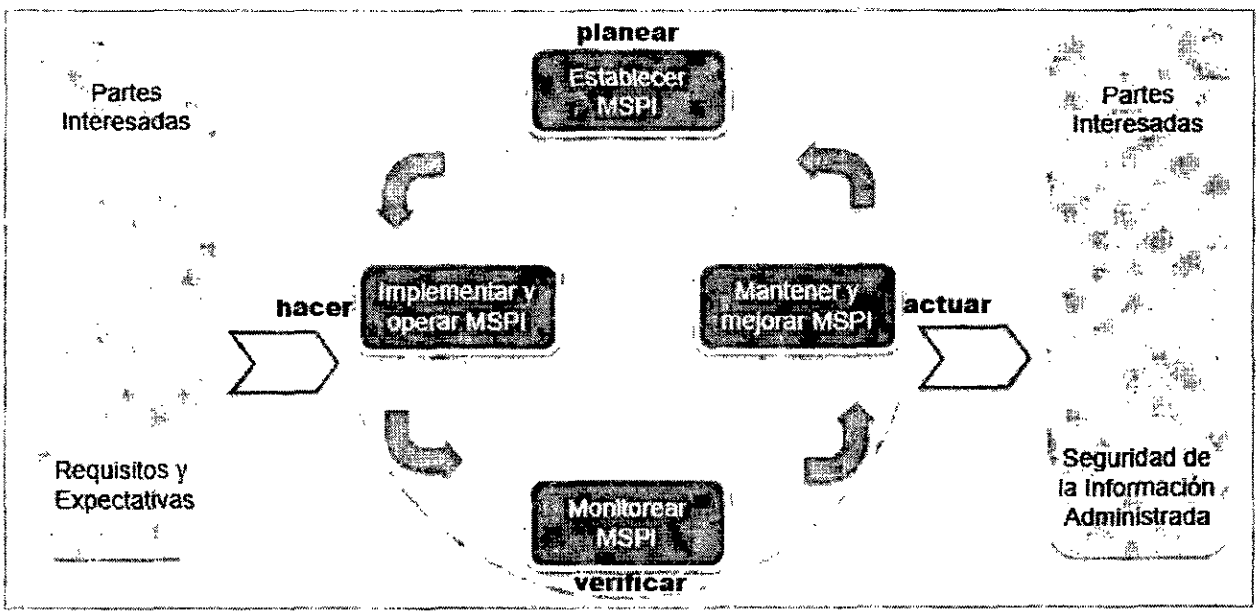
PARÁGRAFO PRIMERO: Todos los procedimientos, manuales y políticas deben ser publicados dentro de la herramienta destinada para la gestión centralizada de documentos institucionales.

ARTÍCULO DÉCIMO SEGUNDO: Objetivos específicos de seguridad de la información[9]. Para cada uno de los controles establecidos en la Norma se deberá establecer la Declaración de Aplicabilidad (SOA por sus siglas en Inglés: *Statement Of Applicability*) que permitan a la Entidad proteger su información.

PARÁGRAFO: La Declaración de Aplicabilidad debe ser implementada de acuerdo con las metas y objetivos relacionados en los Planes Estratégicos de la Entidad.

ARTÍCULO DÉCIMO TERCERO: Modelo de Seguridad y Privacidad de la Información. El FONCEP debe implementar el Modelo de Seguridad y Privacidad de la Información (MSPI) como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información de la Entidad.

PARÁGRAFO: La estructura básica del Modelo de Seguridad y Privacidad de la Información es la siguiente:

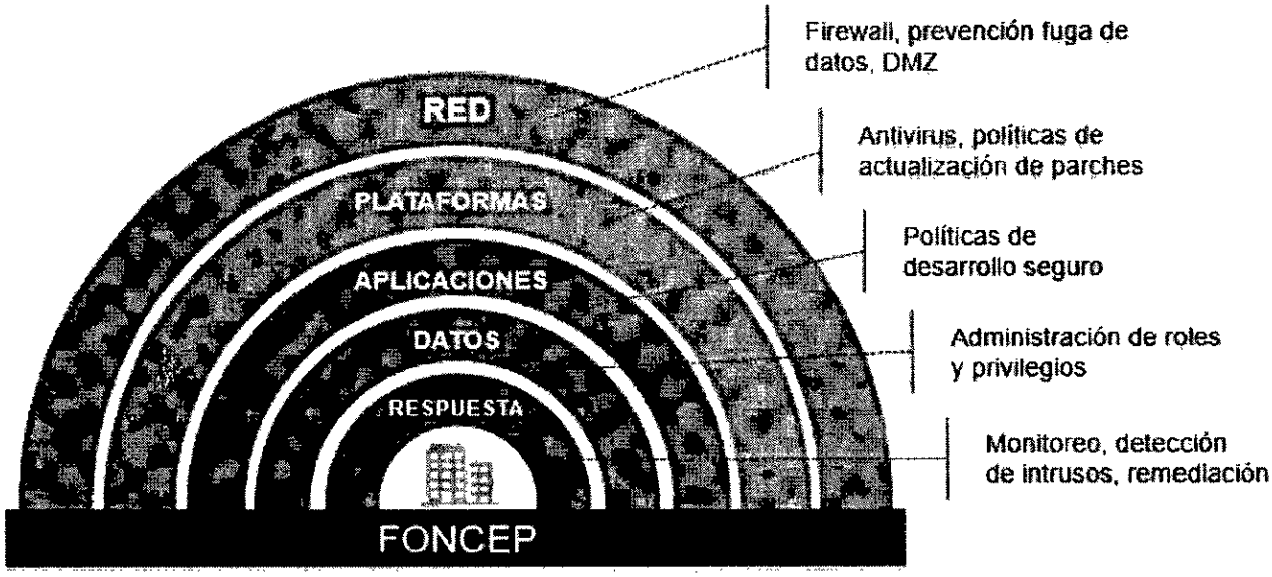


[9] Ver documento DECLARACIÓN DE APLICABILIDAD_V2 en custodia de la Oficina de Informática y Sistemas.

ARTÍCULO DÉCIMO CUARTO: Concepto de Defensa en Profundidad. Bajo la premisa de que todo componente de un sistema puede ser vulnerado, y que el FONCEP no debe delegar la seguridad de un sistema en un único método o componente de protección, el FONCEP debe utilizar distintas técnicas que permitan, al menos, duplicar los elementos de protección para limitar los daños en caso de una intrusión en la primera línea de defensa o componente más expuesto.

ARTÍCULO DÉCIMO QUINTO: Defensa en Capas. La siguiente gráfica ilustra establece los parámetros mínimos para la defensa en capas, estableciendo la red como la capa más externa, denominada protección perimetral, hasta llegar al usuario final, denominado protección *end-point*, caracterizada por la respuesta del equipo de soporte técnico y la protección del PC o portátil:

Defensa en profundidad



CAPÍTULO II. Acerca de la Infraestructura Tecnológica

ARTÍCULO DÉCIMO SEXTO: Datacenter. El FONCEP cuenta con un espacio dotado técnica y ambientalmente para alojar equipos de infraestructura tecnológica denominado Datacenter, construido con base en los mejores estándares reconocidos para la administración y funcionamiento de Centros de Cómputo. Adicionalmente está dotado de los elementos de comunicaciones suficientes que permiten el establecimiento de prácticas de computación en la nube (*cloud computing*).

ARTÍCULO DÉCIMO SÉPTIMO: Características Mínimas del Datacenter. El Datacenter debe tener como mínimo las siguientes características:

1) Incorporar un sistema de alimentación eléctrica con redundancia,

2) Disponer de un sistema de seguridad para el control de acceso,

3) Disponer de una red integrada de cableado estructurado horizontal,

4) Disponer de racks de comunicaciones y de servidores,

5) Disponer de un sistema de acondicionamiento ambiental compuesto por unidades manejadoras de aire acondicionado de precisión.

ARTÍCULO DÉCIMO OCTAVO: Servidores y Almacenamiento. La entidad debe contar con una plataforma segura y robusta con al menos lo siguiente:

- El licenciamiento de diferentes sistemas operativos en servidores (*e.g.* Windows Server 2003, 2008 y 2012),
- Al menos un chasis que consolide los servidores (*e.g.* HPE Blade System C7000),
- Una interconexión de redes,
- Almacenamiento compartido en una única solución que pueda administrarse como un entorno unificado.

PARÁGRAFO PRIMERO: La infraestructura tecnológica debe ser diseñada para que sea bajo demanda sobre ambientes reales y virtuales (*e.g.* VMware y OVM), que permita a la entidad dar la flexibilidad necesaria para proveer las demandas de procesamiento para atender necesidades de operación y nuevos proyectos de TI.

PARÁGRAFO SEGUNDO: La plataforma debe contar con facilidad de virtualización para operar al menos los ambientes de producción y desarrollo.

ARTÍCULO DÉCIMO NOVENO: Herramienta de copia de respaldo a cinta. Se debe contar con una solución de gestión de copias de seguridad (e.g. Backup Exec 2016) la cual estará configurada con unas librerías de LTO, permitiendo copias de seguridad y recuperación eficaces, flexibles y fáciles de usar para ambos entornos: físico y virtual.

ACUERDO DE JUNTA DIRECTIVA No. 010 de 2018

"Por medio del cual aprueba el Manual de Seguridad de la Tecnología de la Información del FONCEP"

ARTÍCULO VIGÉSIMO: El FONCEP debe contar con un ERP compuesto de módulos integrados, todos ellos siguiendo estándares y buenas prácticas de programación segura, que incluye control de acceso y segregación de funciones mediante roles y permisos:

1) **Contabilidad:** Registro y control sistemático de todas las operaciones y movimientos generados en los módulos de gestión, permitiéndole generar información financiera significativa de una forma resumida, ordenada.

2) **Operación y Gestión de Tesorería:** Permite el registro de las operaciones de ingresos y egresos de la Tesorería, así como las respectivas afectaciones contables y presupuestales.

3) **Personal y Nómina:** Administración y control de los funcionarios de planta, soporta los procesos de pago de nómina, control de actos administrativos, bienestar, salud ocupacional y capacitación.

4) **Contratación:** Apoya el Registro y Control de las Etapas de Planeación, Pre-Contractual y Contractual de los procesos de Adquisición de Bienes y Servicios de la Entidad.

5) **Sistema Programa Anual de Caja:** Apoya la programación y reprogramación mensual de los gastos de vigencia, reservas y cuentas por pagar del Presupuesto Distrital.

6) **Sistema de Presupuesto:** Apoya el proceso de ejecución, control y seguimiento del presupuesto de la Entidad.

7) **Sistema de Administración de Elementos de consumo y devolutivos:** Registro de los ingresos, egresos y movimientos de los elementos.

8) **Terceros:** Registra los empleados, contratistas y proveedores que se usan en los demás módulos.

9) **Caja Menor:** Sistema de gestión de la caja menor de la Entidad.

ARTÍCULO VIGÉSIMO PRIMERO: Aplicativos Independientes. Así mismo FONCEP debe contar con aplicativos independientes al ERP que permita la gestión de los procesos misionales y *core* de negocio, entre otros debe contar con al menos los siguientes sistemas de información:

1) Sistema de liquidación de nómina de pensionados.

2) Sistema de liquidación de cuotas parte.

3) Sistema de cobro coactivo.

4) Sistema de bonos pensionales.

5) Sistema de administración de la cartera hipotecaria.

6) Sistema de gestión de comunicaciones y documentos.

7) Herramienta del Sistema de Calidad para planeación anual y gestión de indicadores.

8) Herramienta que permite gestionar los RQ de Mesa de Ayuda.

ARTÍCULO VIGÉSIMO SEGUNDO: Arquitectura de red. La arquitectura de conectividad implementada deberá ser basada en un modelo jerárquico de tres capas donde se cuente con *switches* de acceso, distribución y *core*, este último en alta disponibilidad (HA).

ARTÍCULO VIGÉSIMO TERCERO: Esquema de Servidores. El esquema de servidores tanto virtuales como físicos deberá disponer de redes independientes de pruebas, desarrollo y producción en los ambientes de base de datos y servidores de aplicaciones.

ARTÍCULO VIGÉSIMO CUARTO: Red de Área Local. La red LAN (*i.e. Local Area Network*) de la sede Principal se debe componer de al menos los siguientes elementos:

1) Configuración de la red en topología de estrella con enlaces redundantes.

2) Un *backbone* de fibra óptica multimodal, que interconecte los centros de cableado de cada uno de los pisos o sedes con enlaces de alta velocidad.

3) Incorporar Tecnología de "Enlaces Agregados" que garantizar la interconexión entre los switches de piso y el datacenter (*e.g. equipos HP A5120 y equipos Extreme Networks X440-G2*).

4) Cableado estructurado categoría mínimo 6 y 6A para la comunicación de los equipos de cómputo de usuario final.

5) Switches de piso distribuidos en una topología de estrella que lleguen a un equipo de *core* principal.

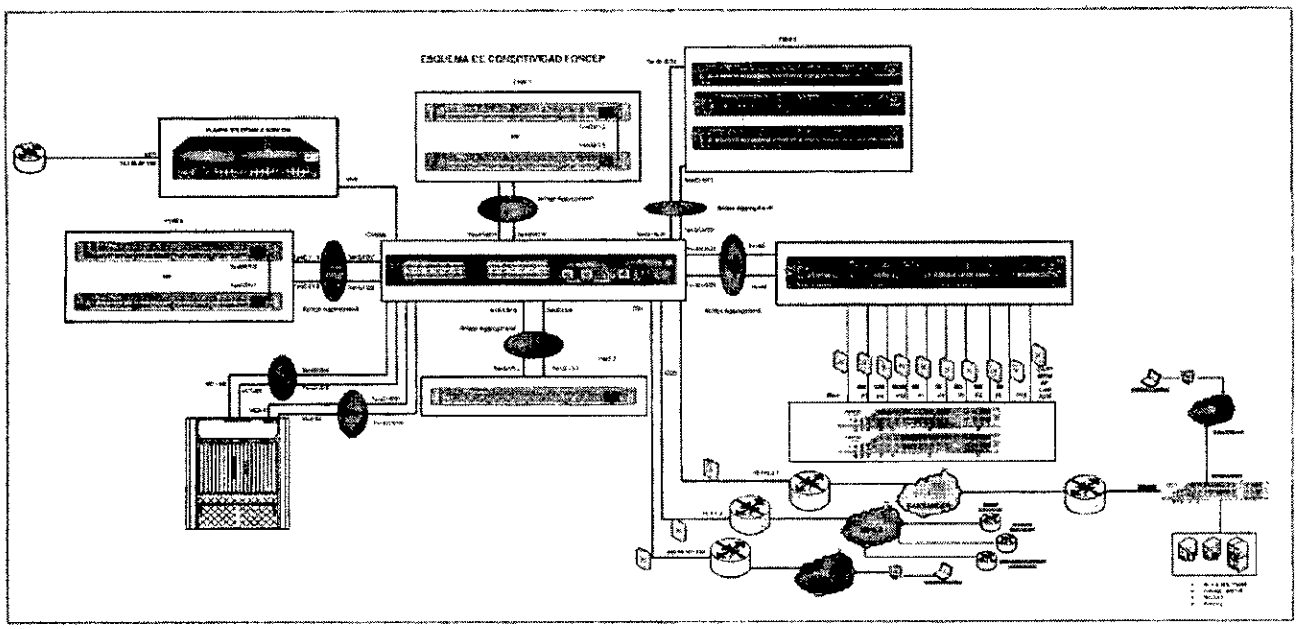
6) La seguridad de red LAN/WAN debe estar compuesta mínimo por dos equipos de seguridad perimetral, con enrutadores para la comunicación a Internet, datacenter alterno y conexión con entidades externas mediante una red MPLS y equipos firewall encargados del aseguramiento de la red perimetral.

7) El establecimiento de la seguridad del acceso remoto se debe garantizar mediante la configuración de redes privadas virtuales VPN, adicionalmente la red debe estar segmentada mediante VLAN con el fin de tener un mejor rendimiento, seguridad y control de tráfico.

8) Para establecer comunicación con puntos remotos donde el FONCEP hace presencia institucional, la sede principal debe contar con un canal dedicado de al menos 8 Mbps, el cual reciba los canales de las sedes.

9) La solución antivirus debe estar respaldada por firmas de última generación reconocidas por la industria.

El siguiente diagrama muestra el modelo general de la arquitectura de red y los diferentes elementos de procesamiento, almacenamiento y conectividad, además de los dispositivos de seguridad dispuestos que deben hacer parte de la infraestructura tecnológica del FONCEP:



ARTÍCULO VIGÉSIMO QUINTO: Transición IPv4 a IPv6. FONCEP en cumplimiento de lo dispuesto en la resolución 2710 de 2017, "Por la cual se establecen lineamientos para la adopción del protocolo IPv6" para el país, debe hacer frente al reto de realizar la transición del protocolo IP (Internet Protocol) versión 4 a la nueva versión 6 (IPv6), con el propósito de garantizar el direccionamiento de dispositivos y aplicaciones que conforman la infraestructura tecnológica, ante el inminente agotamiento de las direcciones disponibles en la versión 4. Los direccionamientos ofrecidos por las dos tecnologías se explican a continuación:

- Las direcciones IPv4 se componen de 32 bits en notación decimal: hasta 232 direcciones.
- Las direcciones IPv6 se componen de 128 bits en notación hexadecimal: hasta 2128 direcciones.

ACUERDO DE JUNTA DIRECTIVA No. 010 de 2018

"Por medio del cual aprueba el Manual de Seguridad de la Tecnología de la Información del FONCEP"

ARTÍCULO VIGÉSIMO PRIMERO: Vigencia. El presente Acuerdo de Junta Directiva rige a partir del día siguiente a la fecha de su expedición.

Dado en Bogotá, D.C., a los 27 días del mes de Julio de 2018.

COMUNÍQUESE Y CÚMPLASE

HÉCTOR MAURICIO ESCOBAR HURTADO
Presidente Junta Directiva

JUAN CARLOS HERNÁNDEZ ROJAS
Secretario Junta Directiva