FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA DE LOS SERVIDORES CIVILES DEL TRÁNSITO NACIONAL FCPC-FONCETRA

PLAN GENERAL TECNOLOGIA 2024

1. OBJETIVO

El presente documento tiene como objetivo, identificar los riesgos tecnológicos y actividades de continuidad de negocio del Fondo, con el fin de garantizar los préstamos quirografarios, prendarios e hipotecarios, estableciendo niveles de responsabilidad al personal clave que integra el FCPC-FONCETRA.

INDICADORES:

$$\frac{\text{No. de mantenimientos de equipos planificados}}{\text{No. de mantenimientos de equipos verificados}}$$

$$\frac{\text{No. de información respaldada planificada}}{\text{No. de información respaldada}}$$

$$\frac{\text{No. de incidentes presentados}}{\text{No. de incidentes resueltos}}$$

2. ALCANCE

El presente plan de tecnología tiene como alcance la identificación y asignación de las tareas, responsabilidades y acciones a tomar, encaminadas a ejecutar decisiones oportunas ante cualquier contingencia que se pudiera presentar como consecuencia de un siniestro.

3. RESPONSABLES

Los funcionarios y empleados que laboran en el FCPC-FONCETRA y que utilicen la infraestructura y / o se encuentren dentro de las instalaciones.

1.1 **Representante Legal**
1.2 **Analista de Crédito y Prestaciones**
1.3 **Contadora General**
1.4 **Abogado Externo**
1.5 **Auditor Interno**
1.6 **Soporte Informático**

4. COMISION DE TECNOLOGIA DE INFORMACION Y COMUNICACIONES

En la actualidad es muy importante impulsar el Desarrollo Tecnológico, con la finalidad de crear un instrumento esencial en el soporte de los procesos de Negocio y generar valor a los servicios que se prestan, así como el manejo de la información generada por las áreas de la entidad. Por tal razón, se consideró de vital importancia la creación de una Comisión de Tecnología de Información y Comunicaciones, que atiende las necesidades del negocio con criterios de racionalidad, austeridad y disciplina presupuestaria; políticas y normas de eficiencia y productividad, que coadyuva en la coordinación de los servicios informáticos que permite estudiar y dar seguimiento a los diversos programas y planes o acciones de desarrollo.

Su principal Objetivo es Diseñar y mantener actualizado el ***Plan General de Tecnología 2024,*** estableciendo los estándares administrativos y tecnológicos que faciliten que la estrategia de negocio y las prioridades se vean reflejadas en los planes tácticos de TI, los cuales establecen objetivos, planes y tareas específicas, entendidas y aceptadas tanto por el fondo como por TI.

La Comisión de Tecnología de Información y Comunicaciones, tiene en su cronograma reuniones periódicas efectuadas y trimestralmente, con el fin de planificar el trabajo y las tareas mensuales, aquí se generan actas de cada reunión donde se identifican tareas y responsables con plazos definidos.

La comisión está integrada por:

Representante Legal: Ing. Dilmer Alejandro Palacios Moncayo

Contadora General: Ing. Delia Viviana Paucar Pillalaza

Soporte Informático: Ing. Rolando Sebastián Rodríguez Ribadeneira

5. INFRAESTRUCTURA

5.1. CENTRO DE COMPUTO

Centro de cómputo, **centro de procesamiento de datos**, **centro de datos o data center** es la entidad, oficina o departamento que se encarga del procesamiento de datos e información de forma sistematizada. El procesamiento se lleva a cabo con la utilización de computadoras que están equipadas con el Hardware y el Software necesarios para cumplir con dicha tarea, las mismas que se encuentran interconectadas en Red y cuentan con conexión a Internet. Este debe contar con la infraestructura adecuada para salvaguardar los equipos en el instalado.

Situación actual:

El FCPC-FONCETRA utiliza la infraestructura informática de las instalaciones de la ANT, ubicado en la Avenida Antonio José de Sucre y José Sánchez, misma que cuenta con un centro de cómputo, cableado estructurado, tomas reguladas, red telefónica. La conectividad hacia internet es privada.

5.1.2 RIESGOS ENCONTRADOS

- Dependencia de Infraestructura
- Acometida eléctrica independiente
- Sistema de enfriamiento
- Sistema contra incendios
- Accesibilidad
- Seguridad

Todos los riesgos descritos anteriormente serian minimizados con el adecuamiento del área correspondiente siguiendo las normas.

Amenazas y medidas de seguridad en el área													
Amenaza	**Medidas de Seguridad**												
Debidas al Entorno	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**J**	**k**	**l**	**m**
Fuego	x	x	x	x	x		x				x	x	
Terremoto	x	x		x	x		x				x		
Tormentas	x	x		x	x		x				x		
Inundación	x	x		x	x		x				x		
Fallo de Energía			x	x			x						
Fallo aire acondicionado				x			x						
Debidas al Hombre	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**J**	**k**	**l**	**m**
Daños malintencionados	x	x	x	x	x	x		x	x	x			x
Fraude								x		x	x	x	x
Malversación								x		x	x	x	x
Robo			x		x			x	x	x	x	x	x
Uso NO autorizado de recursos			x		x			x	x	x	x	x	x
Sabotaje / Espionaje			x	x	x			x		x	x	x	x
Daños Fortuitos				x							x	x	x

Claves	
a. Diseño del edificio	h. Control de acceso al sistema
b. Construcción del edificio	i. Aseguran. De ventanas y puertas
c. Colocación dispositivos detección	j. Programa de selección de personal.
d. Identificó. Y prueba equipo backup	k. Adhesivo a auditorias, medios de registro y proc. de control.
e. Sistema aviso bomberos/policía	l. Estándares y procedimiento documentados
f. Backup de energía/ aire acondicionado	m. Formación y entretenimiento de personal

5.2 CONTROL DE HARDWARE

A continuación, se muestran tareas realizadas periódicamente con el fin de mantener a punto el Hardware existente dentro del FCPC-FONCETRA.

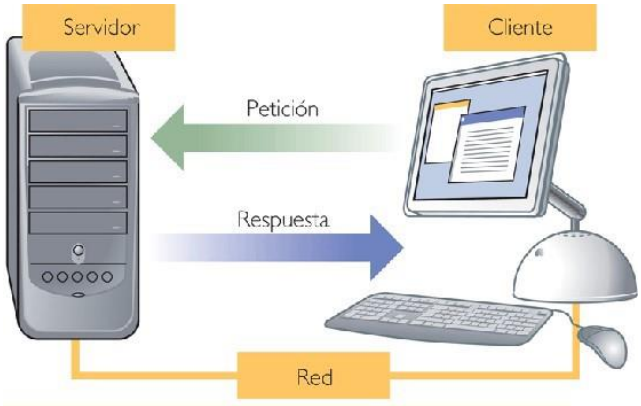
5.2.1 **Inventarios de Equipos**: Control del activo y su ubicación física, responsables del equipo, periféricos (Mouse, Teclado, impresoras, escáner)

5.2.2 **Optimización de equipos:** El correcto uso del hardware, monitoreo por uso de aplicaciones que puedan desencadenar en fallas de los equipos.

5.2.3 **Mantenimientos programados:** Actividad para realizar una limpieza general de todos los componentes de los equipos para alargar la vida útil.

5.2.4 **Equipos backup:** Equipo en espera, en caso de requerir un equipo por un evento inesperado como robo, perdida, caída, este equipo servirá para que el funcionario no deje de realizar sus actividades diarias.

5.3 SERVIDOR DE APLICACIÓN



Los servidores son los equipos maestros o aquellos equipos que proveen de servicio a ordenadores que se encuentran conectados a dicho servidor a través de una Red. Los servidores a diferencia de los equipos terminales, trabajan **todo el tiempo y prácticamente no tienen descanso**. Es por esta razón, que cada cierto lapso de tiempo es necesario realizar mantenimiento preventivo para mantener el funcionamiento de los servidores lo más óptimo posible y evitar errores o situaciones que puedan mermar el funcionamiento de la red.

5.3.1 POSIBLES RIESGOS

Caída del servicio del servidor de aplicación, lo que ocasionaría que todos los empleados se queden sin este aplicativo o servicio, esto puede ser debido a las siguientes causas definidas por su nivel de impacto:

RIESGO	NIVEL DE IMPACTO	INCIDENCIA
Daño o Vulnerabilidad del Software	ALTO	MEDIA
Daño de Hardware	ALTO	BAJA
Falla eléctrica	MEDIO	BAJA
Ataques de virus	ALTO	BAJA
Espacio insuficiente para procesamiento de información	MEDIO	BAJA

5.3.2 ACCIONES A TOMAR PARA MITIGAR LOS RIESGOS

5.3.2.1 MANTENIMIENTO DE HARDWARE un mantenimiento preventivo adecuado minimizaría los riesgos de daño en el servidor, para lo cual se tiene planificado realizarlo trimestralmente.

Guía para realizar un mantenimiento efectivo a los servidores:

5.3.2.1.1. Preparar el equipo para el mantenimiento

El primer paso para realizar el mantenimiento preventivo a nuestro Servidor, es prepararlo para el proceso de mantenimiento. Para ello, debemos apagar el equipo y desconectarlo de los hubs o los sistemas de conexiones hacia el resto de los equipos de la red.

Una vez que el servidor se encuentre libre de conexiones, es momento de retirarlo del armario o rack en donde se encuentra alojado. Lo colocamos sobre una superficie plana y segura y completamente aislante.

Luego, tocamos una superficie metálica para descargarnos de electricidad estática y comenzar el proceso de mantenimiento de hardware.

5.3.2.2. MANTENIMIENTO DE SOFTWARE

Una vez que conectemos el servidor a una fuente de poder y a un monitor, teclado y mouse, es momento de realizar una actualización completa de software, es decir, actualizar el sistema con la última versión de Windows Server o de Linux Server (actualizaciones o parches) que tengamos o cualquier otro sistema que utilice nuestro servidor. De esta manera, aseguramos que las vulnerabilidades se reducirán al máximo.

Después de actualizar el software del servidor, podemos ejecutar el antivirus de manera Live, completamente desconectados de Internet. Se recomienda que sea una versión actualizada para que pueda detectar cualquier anomalía. Una vez ejecutado y eliminadas las amenazas, si las hubiesen, procedemos a realizar una limpieza de archivos temporales. Es momento de apagar el equipo y retirar la fuente, el monitor y demás implementos que utilizamos para el paso anterior y preparar el equipo para conectarlo nuevamente a la red.

5.3.2.2.1 MANTENIMIENTO DE BASES DE DATOS

Actualmente, se está realizando de forma semanal conjuntamente con la extracción del BackUp total de la Base con ayuda del proveedor de aplicación, revisión de logs, indexación.

5.3.2.2.2 CRONOGRAMA DE MANTENIMIENTOS

Actualmente se realiza un mantenimiento de Hardware de forma trimestral tratando de minimizar los riesgos e impacto que esto produce ya que tenemos que bajar el servicio mientras este dure.

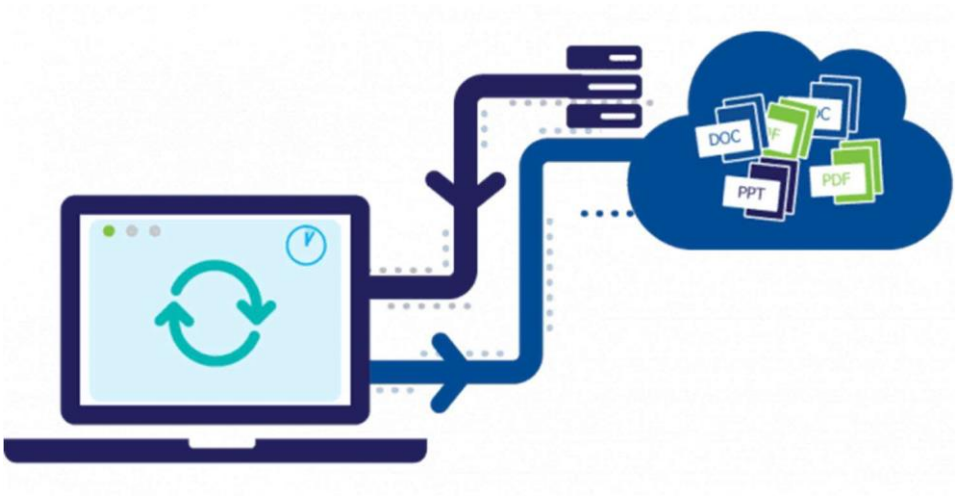
CRONOGRAMA MANTENIMIENTOS		
NUMERO	**TRIMESTRE**	**FECHA PROGRAMADA**
1	PRIMERO	HASTA EL 31 MARZO DEL AÑO EN CURSO
2	SEGUNDO	HASTA EL 30 JUNIO DEL AÑO EN CURSO
3	TERCER	HASTA EL 30 SEPTIEMBRE DEL AÑO EN CURSO
4	CUARTO	HASTA EL 31 DICIEMBRE DEL AÑO EN CURSO

Fechas tentativas

6. REDES Y COMUNICACIONES

Actualmente se tiene contratado el servicio de internet con la empresa Punto Net con un ancho de Banda de 20 Mbps, el cableado estructurado de la red interna está dirigido hacia el Router, las estaciones de trabajo cuentan con puntos de datos 1 a 1.

7. RESPALDOS DE INFORMACION



Una **copia de seguridad** o ***backup en*** tecnología de la información o informática es eld - o el proceso para realizar una copia exacta, con el fin de que estas copias adicionales puedan utilizarse para restaurar el original después de una eventual pérdida de datos. Fundamentalmente son útiles para tres cosas:

Primero: recuperarse de una catástrofe informática.

Segundo: recuperar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente o corrompido.

Ya que los sistemas de respaldo contienen por lo menos una copia de todos los datos que vale la pena salvar, deben de tenerse en cuenta los requerimientos de almacenamiento. La organización del espacio de almacenamiento y la administración del proceso de efectuar la copia de seguridad son tareas complicadas. Para brindar una estructura de almacenamiento es conveniente utilizar un modelo de almacenaje de datos.

Antes de que los datos sean enviados a su lugar de almacenamiento se lo debe seleccionar, extraer y manipular. Se han desarrollado muchas técnicas diferentes para optimizar el procedimiento de efectuar los backups. Estos procedimientos incluyen entre otras optimizaciones para trabajar con archivos abiertos y fuentes de datos en uso y también incluyen procesos de compresión, cifrado, y procesos de duplicación, entendiéndose por esto último a una forma específica de compresión donde los datos superfluos son eliminados. También es importante reconocer las limitaciones y los factores humanos que están involucrados en cualquier esquema de backup que se utilice. Las copias de seguridad garantizan dos objetivos: **integridad y disponibilidad**

7.1. POLITICAS DE RESPALDOS DE INFORMACION DE USUARIOS

Todos los empleados del Fondo son responsables de generar el backup personal de su información para lo cual el fondo les ha dotado de una cuenta de G-suite misma que presta la herramienta DRIVE con una capacidad personal de 30 GB donde deberán respaldar suinformación de forma segura y con fácil acceso.

Por otro lado, se realiza un BackUp de forma mensual que es extraído a un disco externo con la información importante de cada uno de los usuarios y es almacenado fuera del Fondo.

7.1.1 POLITICA PARA LA REALIZACION DE RESPALDOS

A continuación, se detalla el procedimiento a seguir para realizar un backup de los archivos importantes (no fotos, mp3, videos, etc.) para los equipos de trabajo del Fondo.

7.1.2.1 **Carpeta "Mis Documentos"** aquí deberá guardarse toda la información importante de su trabajo que tenga relación con el fondo. Se tomará el backup solo de esta carpeta, por lo que los usuarios deberán colocar y manejar aquí sus archivos.

7.1.2.2 **Sugerencia:** cada usuario deberá crear carpetas dentro de "Mis Documentos" a fin de organizar la información y en caso de necesitarse restaurar algún archivo ubicarlo fácilmente. Estos son algunas recomendaciones:

Recomendación 1

Crear carpetas de acuerdo al tipo de archivo que estén manejando, así: carpeta

- **Word:** aquí deberán almacenarse los archivos que se creen con este aplicativo
- **Excel:** almacenar plantillas, archivos elaborados con esta herramienta (*.xls)
- **Power Point:** almacenar las presentaciones
- **Correo:** colocar aquí el backup de su correo

Recomendación 2

- Crear carpetas según sea el caso para discriminar otros tipos de archivos (ejemplo: visio, project, etc.)

7.1.2 **Respaldo de Correo**, todos los empleados cuentan como herramienta de correo con una cuenta de g-mail corporativa, misma que cuenta con una gran capacidad de almacenamiento y respaldo automático por encontrarse en la nube

7.1.3 **Información,** hasta tanto no se realice la estandarización e unificación de los documentos en la carpeta “Mis Documentos” de cada usuario, el paso o copia de los archivos a ser respaldados son responsabilidad de cada uno de los usuarios

7.1.4 **Calendario de Respaldos,** se recomienda hacer un backup de su información como considere cada usuario, pero obligatoriamente el último día laborable de cada mes.

7.2 POLITICA DE RESPALDO DE LA BBDD EN LA NUBE

7.2.1 NECESIDAD

El FCPC-FONCETRA dispone de un sistema Administrativo-Financiero compuesto por una interfaz de acceso y una base de datos, misma que se viene respaldando de forma física en discos duros semanalmente. El Fondo, ha visto la necesidad de generar un respaldo adicional de esta información y de los respaldos que se generen a futuro, en un servidor fuera de las instalaciones del FCPC-FONCETRA, con niveles de seguridad y disponibilidad mayores.

7.2.2 SOLUCION IMPLEMENTADA

a) Se genera un respaldo de la base de datos de la aplicación administrativo-Financiera, los días viernes de cada semana, salvo en el caso en que no se labore en el Fondo.
b) Se almacena el respaldo obtenido en la nube, en un servidor remoto.
c) Se dispone un acceso remoto vía FTP al repositorio, con las seguridades respectivas.

8. SEGURIDAD DE LA INFORMACION

8.1 POLITICAS DE CONTRASEÑAS SEGURAS

Los usuarios del FCPC-FONCETRA seguirán las siguientes normas en cuestión de manejo de contraseñas:

8.1.1 GENERACION DE CONTRASEÑAS SEGURAS:

- Será cambiada con una periodicidad mensual.
- Generación de clave fácil de recordar, no de detectar.
- Contiene al menos 10 caracteres incluyendo mayúsculas, minúsculas, números y símbolos.
- Cuidar la visibilidad al momento de la escritura de la clave.
- No es posible compartir claves ni solicitar la de otros funcionarios.
- Está prohibido escribir la clave de acceso al equipo en papeles ni guardarlos en archivos sin protección.
- Si por algún motivo tuviere que escribir la clave, no dejarlo al alcance de terceros, debajo del teclado, en un cajón del escritorio, pegado en el computador, etc.
- Está prohibido habilitar la opción, recordar contraseña en los programas utilizados.
- Está prohibido el envío de claves de usuario por correo, chat o teléfono.
- Sera responsabilidad del usuario bloquear su equipo cuando se ausente de su estación de trabajo.

El incumplimiento a estas normas y políticas serán sancionadas de acuerdo a lo establece el reglamento interno de trabajo.

8.2 POLITICA DE CONFIDENCIALIDAD

Todos los usuarios internos y externos (proveedores) del fondo deberán firmar en su contrato una cláusula de confidencialidad, como la que se muestra a continuación:

“PROHIBICIONES

Si durante el transcurso del presente contrato, llegará a conocimiento del **Empleado o funcionario** información privilegiada o confidencial, que comprende, sin limitar a la relacionada con propiedad intelectual, secretos industriales, software de computación, patentes, planificación estratégica y operacional, planes de mercado, publicidad o producción, finanzas, operaciones o asuntos de negocios,

estrategias, fusiones, adquisiciones y/o cualquier operación o asunto de negocios, ya sea de manera verbal, escrita, magnética, o por cualquier otro medio, éste tendrá prohibido el uso y divulgación de la información privilegiada o confidencial en asuntos que no sean los relacionados a la prestación de los sus servicios al **Fondo**, mientras duren éstos y después de ellos.

El EMPLEADO declara expresamente que conoce las consecuencias civiles y penales que el incumplimiento de esta cláusula acarrea."

9. SOPORTE TECNICO

En función de las necesidades planteadas para el FCPC-FONCETRA donde el giro de su negocio no está enfocado para tener un departamento de sistemas, ya sea por el número de usuarios como es el caso del Fondo o por el número de aplicaciones, lo recomendable es que una entidad externa sea la responsable en llevar el control del área de tecnología y que este sea medida por incidentes o requerimientos y estos a su vez por métricas de niveles de acuerdo de servicio, en atención y/o resolución.

El riesgo de no contar con un servicio externo y formalizar la metodología de soporte puede llevar a contar con un servicio no cuantificable y no medible, por lo cual este es una debilidad con la que cuenta el Fondo.

En este sentido el Fondo tiene contratado los servicios profesionales de un especialista de TI, mismo que presta su contingente.

A continuación, definimos algunos términos a ser utilizados para el manejo del soporte necesario

- **Requerimiento:** Solicitud relacionada con una consulta o soporte técnico, funcional y operativo de software, hardware y servicios, ingresado por los usuarios finales.

- **Incidente:** Interrupción no planificada de un servicio de TI o una reducción de la

calidad de un servicio de TI.

- **Soporte Técnico:** en este caso es el especialista de TI contratado bajo la modalidad de servicios profesionales, quien es el encargado de brindar el soporte de primer nivel

- **Especialista Primer Nivel (N1):** Se denomina primer nivel al grupo de soporte de encargado de establecer un primer contacto con el usuario, encontrando soluciones al requerimiento generado y/o escalarlo a los siguientes niveles de soporte, realizando el adecuado seguimiento de la solución hasta su cierre.

- **Especialista Segundo Nivel (N2):** Se denomina segundo nivel al grupo de soporte de la MST y otras áreas de tecnología que apoyan a la MST en la solución de requerimientos generados para este nivel y que no pueden ser resueltos en el primer nivel. En este nivel participarían los proveedores de los servicios hasta la resolución.

10. CONTINUIDAD DEL NEGOCIO

La continuidad del negocio es el nivel de preparación que tiene EL FCPC-FONCETRA para mantener las funciones esenciales tras una emergencia o una interrupción. Estos eventos pueden incluir vulneraciones de seguridad, desastres naturales, cortes de energía, averías de los equipos o la salida repentina de un empleado clave.

10.1 GLOSARIO DE TÉRMINOS

- **Riesgo Operativo:** Es la posibilidad de que ocurran pérdidas como consecuencia de una falla, deficiencia o inadecuación de procesos internos, personas, sistemas o **eventos externos**.
- **Procesos Críticos:** Son aquellos que de alguna forma hacen que el negocio siga funcionando.
- **Eventos Externos:** Pérdidas procedentes de eventos ajenos al control de la entidad y que pueden alterar el desarrollo de su actividad.
- **Teletrabajo:** Es la prestación de servicios lícitos y personales, con relación de dependencia, de carácter no presencial, en jornadas ordinarias o especiales de trabajo, fuera de las instalaciones del lugar donde labora.
- **Estado de excepción:** Es un mecanismo contemplado en la legislación de un país para afrontar situaciones extraordinarias y graves, que incluye mayores poderes para el Gobierno.
- **Toque de queda:** Es la prohibición o restricción, establecida por instituciones gubernamentales, de circular libremente por las calles de una ciudad y/o permanecer en lugares públicos o privados.
- **C.O.E.:** El Centro de Operaciones de Emergencias (COE), es un componente del Sistema Nacional para Emergencias y Desastres, responsable de promover, planear, y mantener la

coordinación y operación conjunta, entre diferentes niveles, jurisdicciones y funciones de instituciones involucradas en la RESPUESTA y/o ATENCION de eventos naturales o antrópicos adversos.

10.2. PLAN DE CONTINUIDAD DEL NEGOCIO

El desarrollo e implementación de los planes de continuidad se realizarán considerando los escenarios de indisponibilidad de Instalaciones, Equipos, Tecnología, Recurso Humano y Proveedores.

La Comisión de Tecnología en sus reuniones trimestrales definirá estrategias para la continuidad del negocio en base a la situación actual y tomando en cuenta disposiciones y recomendaciones del Comité de Operaciones de Emergencia - COE Nacional, órgano administrador BIESS y de control Superintendencia de Bancos.

Para esto el Fondo se ha asegurado de:

- Aplicar las políticas y programas de capacitación/entrenamiento permanente para el personal responsable de la continuidad y sus delegados.
- Establecer esquemas de trabajo.
- Establecer modalidad de trabajo.
- Contar con un esquema específico de comunicación.
- Identificar y desarrollar las estrategias de continuidad.
- Contar con garantías necesarias para la continuidad del negocio.
- Diseñar, implementar y probar los planes de recuperación de sus procesos.
- Monitorear el funcionamiento del Plan de Continuidad del Negocio.

10.2.1 ORGANIGRAMA FUNCIONAL E IDENTIFICACION DE EMPLEADOS CLAVE

- **NIVEL EJECUTIVO**

  GERENTE GENERAL O REPRESENTANTE LEGAL DEL FONDO

- **NIVEL ADMINISTRATIVO**

  ANALISTA DE CRÉDITO Y PRESTACIONES

  CONTADOR/A GENERAL

- **NIVEL ASESOR**

  ASESOR JURIDICO

  AUDITORÍA INTERNA/EXTERNA

  ESPECIALISTA TI

10.2.2 DOTACION DE EQUIPOS

Todos los empleados identificados como clave cuentan con el soporte necesario en caso de una contingencia o desastre en cuestión de equipos de computación al igual que cuentan con un equipo portátil (laptop) con los accesos necesarios a la información del Fondo.

10.2.3 ACCESO A INFORMACION Y COPIAS DE SEGURIDAD

El Fondo cuenta con copias de seguridad de la información o BackUps tanto de usuarios como de la BBDD del sistema. Los usuarios identificados como clave cuenta también con acceso a su backup personal almacenado en la nube en la herramienta Drive de Google con disponibilidad desde donde se encuentren físicamente los 365 días del año. Este acceso cuenta con las seguridades respectivas.

10.2.4 INFRAESTRUCTURA PARA REALIZAR TELETRABAJO

Se encuentra configurado el acceso remoto hacia el fondo utilizando las herramientas ANYDESK y Team Viewer para cada uno de los usuarios claves, con esto en caso de necesitar conectarse para realizar teletrabajo lo pueden hacer de forma adecuada.

10.2.5 COMUNICACIÓN CON PERSONAL DEL FONDO

El personal del Fondo cuenta con las herramientas tecnológicas corporativas como ZOOM y HangOuts para realizar reuniones, videollamadas o chats y de esta forma interactuar en caso de ser necesario.

10.2.6 COMUNICACIÓN CON LOS PARTICIPES Y SITIO DE CONSULTA

El Fondo cuenta con la página Web www.foncetra.fin.ec donde constantemente se publican noticias y resoluciones importantes para conocimiento de los partícipes. De igual forma desde esta herramienta cada participe puede consultar su estado de cuenta de saldos, para lo cual se le configuro un usuario y contraseña personal.

11. DISEÑADO Y ELABORADO POR:

Ing. Rolando S. Rodríguez R.