

Formulario COVID CYBER

Salud financiera / operativa general

1. ¿Cómo ha impactado la pandemia del COVID-19 en las operaciones de la organización?

Rta. El impacto fue mitigado con el trabajo en casa y con la habilitación por medio de acceso remoto a todos los servicios, aplicaciones y sistemas de comunicación, permitieron ejecutar todas las operaciones del Fondo, sin interrupción, incumplimientos o algún tipo de pérdida. Para habilitar la ejecución de algunas operaciones en medios totalmente digitales se ajustaron formatos y flujos de información haciendo uso del gestor documental.

2. ¿Qué cambios se han realizado en el presupuesto con relación a los departamentos que no generan ingresos (por ejemplo: Tecnología, Recursos Humanos, Legal)?

Rta. Ninguno

3. ¿Cuál es la capacidad de la organización para pagar la deuda / capacidad para refinanciar deuda u obtenerla?

Rta. La entidad no tiene obligaciones por deudas económicas

4. ¿Dónde ve la organización la exposición para un posible reclamo de un cliente o un tercero? ¿Cuenta con alguna exposición que pueda generar una reclamación relacionada con el COVID-19?

Rta. Del análisis de riesgos realizado por el impacto del covid19 no se identificó alguna condición, causa, vulnerabilidad que no fuera tratada y que pudiera llevar a algún incumplimiento de las obligaciones, servicios o tramites que presta el Fondo y en consecuencia alguna afectación por reclamos de terceros o clientes.

Estándares contractuales y de servicio

1. ¿Se han alterado alguna de las disposiciones estándar en los contratos o servicios ofrecidos al cliente? ¿acuerdos en el futuro? ¿Han realizado algún acuerdo con clientes que han sido particularmente útiles para abordar el impacto de COVID-19 en sus servicios?

Rta. Todos los servicios prestados por contratistas al Fondo que implicaron contactos presenciales fueron atendidos de manera virtual. No se presentó alteración de dichos servicios. Se tenían previstas capacitaciones a cooperativas de manera presencial, estas se realizaron de manera virtual. Todos los tramites oficiales que presta el Fondo están habilitados para ser ejecutados por medios digitales, estos son: Recaudo de Prima de

Seguro de Depósitos, Pago del seguro de depósitos, el cual fue revisado y ajustado para asegurar que se ejecutará totalmente en línea: los demás tramites oficiales inscripciones y operaciones e apoyo no se han presentado desde el inicio del periodo Covid19 hasta la fecha. Los demás servicios y trámites administrativos se realizaron por medios digitales.

2. ¿Cómo está alterando el entorno actual (Pandemia), la forma en la que la organización cumple con los acuerdos de servicio existentes?

Rta. El efecto de la pandemia alteró el contexto en que ejecuta la entidad sus operaciones, llevándola a ajustar sus flujos de información interna, ejecución de procesos y prestación de servicios por medios digitales.

Continuidad del negocio / Teletrabajo

1. ¿Cómo es la gestión de riesgos de la organización en cuanto a procesos? ¿Cuentan con un departamento involucrado en temas relacionados al COVID-19? ¿Cómo está la planificación del plan de continuidad del negocio y las pruebas de recuperación ante desastres, teniendo en cuenta los nuevos escenarios que surgen a raíz de la pandemia?

Rta. El plan de continuidad del negocio se actualizó en II semestre de 2021. Se revisaron los riesgos de continuidad y a partir de estos se identificaron los escenarios de desastre, incluido en estos temas sanitarios y de pandemias. Para cada escenario se tienen definido estrategia de continuidad, entre ellas el DRP el cual se encuentra en proceso de implementación (replica de la infraestructura, servicios, aplicaciones en datacenter alterno en Cali-Valle). El tema sanitario y el protocolo de bioseguridad es administrado por los responsables del sistema de seguridad y salud en el trabajo y de gestión del Talento Humano. El comité de crisis o de emergencia fue instaurado para tratar el impacto de la emergencia y la operatividad de la entidad.

2. ¿Cuáles son las implicaciones del trabajo remoto para su organización y las implicaciones en la eficiencia operativa?

Rta. El acceso remoto habilitó los servicios de TI, aplicaciones, servicios de comunicación y demás recursos para ejecutar todos los procesos del Fondo. El trabajo remoto para todo el personal se habilitó mientras estuvo vigente la emergencia sanitaria y en consecuencia el trabajo en casa. A partir del 1 de julio de 2022 se terminó la emergencia sanitaria y el acceso remoto se habilita para casos particulares que requieren realizar trabajo.

3. ¿Cómo es la recuperación de la organización ante algún desastre o incidente?

Rta. Los escenarios de desastre identificados y estrategias de continuidad son los siguientes:

Escenarios de Interrupción y estrategias de continuidad



Estrategia de Recuperación	Escenarios					
						
	E1. Interrupción total de servicios tecnológicos en Centro de Cómputo FOGACCOOP.	E2. Interrupción total de servicios tecnológicos en Datacenter Principal (LUMEN)	E3. No disponibilidad de las oficinas administrativas de FOGACCOOP (Sede A y Sede B)	E4. Ausencia Masiva de Personal Clave (Pandemia y/o epidemias; ausencia de personal competente)	E5. Movilidad restringida de funcionarios y/o proveedores por manifestaciones en el país.	E6. Indisponibilidad de proveedores claves
A1. Centro Alterno Operativo (Interno)			●		☑	
A2. Trabajo desde Casa	●		●	●	●	
A4. Entrenamiento cruzado y líneas de sucesión				●		
A5. Outsourcing de Personal Temporal				●		
A6. Diversificación de proveedores					●	●
A7. Exigencia de prácticas de continuidad a proveedores					●	●
A8. Centro de Computo DRP - Hot site (LUMEN)		●				

4. ¿Cómo se ha visto afectada la cadena de suministro de la organización?

Rta: Los servicios contratados por el Fondo se mantuvieron activos y vigentes durante la emergencia sanitaria. No se presentó alteración de dichos servicios.

Proveedores:

¿Qué tipo de proveedores se utilizan para satisfacer las necesidades de trabajo remoto?
¿Qué tipo de servicios están proporcionando?

Rta:

- Servicio de **DATACENTER Externo (CENTURY LINK)**
- Durante la emergencia se celebró contrato de arrendamiento de equipos portátiles. Con esto todos los funcionarios tuvieron equipos provistos por el Fondo. A la fecha el Fondo adquirió PC portátiles. Se encuentra en proceso de asignación estos PC portátiles para todo el personal de la entidad. (NEX COMPUTER S.A.S - COMPUFAST PREMIUM S.A)
- Suscripción Office365 (SOLUCIONES ORION SUCURSAL COLOMBIA).

1. ¿Cuántos y cuáles de sus proveedores críticos han tenido un impacto significativo en sus operaciones, a raíz de la pandemia, generando una reducción en SLA (Acuerdo de Nivel de Servicio) a la organización? ¿Cuentan con reemplazos para estos?

Rta. Ninguno de los proveedores críticos del Fondo (Datacenter, Proveedor de red local, proveedores de soporte de aplicativos, proveedores de precios para valoración del portafolio, entidades bancarias, ACH, entre otros) presentó alteración de sus ANS u obligaciones con el Fondo a raíz de la pandemia.

2. ¿Cómo está revisando el proceso contractual la organización? (Teniendo en cuenta la situación del COVID-19)

Rta. El proceso no sufrió cambios sustanciales, excepto en su operatividad interna y flujo de información, la cual migró totalmente a medios digitales. Para el efecto se ajustaron formatos, se hizo uso del gestor documental, se configuraron firmas digitales y electrónicas en contratos y documentos, de conformidad con el alcance que dan las disposiciones legales.

Data Breach:

1. Describa el esquema de todos los accesos remotos que requieren MFA (Autenticación de Múltiple Factor)

Rta: El acceso remoto para trabajo en casa se habilita a través de una VPN. En este sentido se requiere:

Acceso a VPN con usuario y contraseña

Acceso a escritorio remoto con usuario y contraseña

Acceso a aplicativos con usuarios y contraseñas

En conclusión se cuenta con diferentes puntos de control de acceso.

2. ¿Quién es el proveedor de VPN? ¿ha sido totalmente actualizado el servicio?

Rta: DATACENTER EXTERNO (CENTURY LINK)

3. En caso de ataques de puerto(s) RDP, ¿El equipo de IT está preparado para responder frente a estos ataques analizando la configuración de seguridad de los puertos abierto?

Rta: SI- Se tiene un servicio de Seguridad Gestionada y SOC

4. ¿Puede la organización continuar invirtiendo recursos para el fortalecimiento de los controles tecnológicos actualmente implementados?

Rta: La entidad realiza periódicamente análisis de vulnerabilidades y análisis de riesgos a partir de los cuales se identifican necesidades de nuevos controles tecnológicos; de otra parte se realiza evaluación de infraestructura conjuntamente con Datacenter de los cuales resultan recomendaciones sobre nuevos controles de seguridad: todos los requerimientos que demandan recursos se incorporan dentro del presupuesto de gastos que se presenta para aprobación a Junta Directiva.

Interactividad del usuario

1. ¿Se han implementado herramientas para facilitar la comunicación interna de los colaboradores? (Como ejemplo, ¿ahora usan una herramienta de mensajería interna como Teams – Zoom - Slack?)

Rta. La comunicación interna y externa se realiza por medio de la herramienta TEAMS

Interrupción De Negocio

1. ¿La disponibilidad de red de la organización se ha vuelto más relevante para acceder a los servicios corporativos?

Rta.: La red de la organización mantiene los mismos estándares de disponibilidad. Al igual que la disponibilidad de los servicios del Datacenter. Aunque se reconoce su gran importancia para soportar la operatividad de la entidad.

2. ¿El entorno de la organización está construido para la FMH (Trabajo desde casa) para toda la mano de obra a nivel regional / global?

Rta. Si, está construida para soportar las actividades de todos los procesos de la entidad, excepto claro está los que fundamentalmente requieren manualidad y presencialidad como la administración del archivo físico y mantenimientos de equipos e instalaciones físicas.

3. ¿Cuáles son los impactos para la organización y la planificación en caso de un posible corte de tecnología? ¿Dualidad, backups u otros?

Rta.

Activar el DRP previsto en datacenter alterno en Cali – Valle

Ejecutar planes de contingencia particulares de servicios, aplicativos y procesos críticos

Restaurar los Backups de información

Ejecutar el Plan de continuidad conforme el RTO y RPO definido por el BIA

4. ¿De qué aplicaciones tecnológicas depende la organización para el trabajo remoto?
¿Conocen las vulnerabilidades en las versiones de esas herramientas?

Rta. _

- *VPN con usuario y contraseña*
- *Escritorio remoto*
- *Computadores portátiles para los funcionarios*

5. ¿La operación de la compañía depende de sus proveedores de tecnología? ¿Cuáles?

Rta.

- *DATACENTER EXTERNO*
- *Proveedores de soporte y mantenimiento de aplicaciones misionales*

Extorsión de red:

1. ¿Han implementado herramientas de seguridad de red con el fin de mitigar las amenazas de Ransomware?

Rta.

- ENDPOINT
- IPS
- WAF
- FIREWALL

Se suscribe el 11 de octubre de 2022.

MARÍA ELENA GRUESO RODRÍGUEZ
Directora – Representante Legal