El Fondo Mundial

Ref.: Asegurar sus sistemas: ciberataques y transacciones financieras fraudulentas durante la COVID-19

Estimados colegas,

La escala e intensidad de los ciberataques y las transacciones financieras fraudulentas están aumentando rápidamente durante la crisis actual. Con un crecimiento exponencial de la actividad en línea, los delincuentes encuentran maneras cada vez más ingeniosas de interceptar información vital y desviar las transacciones financieras.

Incluso una desviación menor respecto de la diligencia debida estándar en los procesos relativos a pagos y desembolsos podría provocar de manera involuntaria una pérdida financiera importante.

En el marco de la nota informativa sobre intercambio de información y gestión de datos del Fondo Mundial, emitida en abril pasado, se ha solicitado a los RP que lleven a cabo las actualizaciones necesarias de sus procesos internos y confirmen cuándo se han ejecutado.

Como un recordatorio de buenas prácticas para RP, SR y receptores de financiamiento del MCP, deben ceñirse a las mejores prácticas siguientes:

- Adoptar la actitud de "**Nunca confiar, siempre verificar**" respecto de todas las transacciones financieras. Las solicitudes más peligrosas son con frecuencias las que parecen provenir aparentemente de una dirección o un número telefónico que conocemos bien. En algunos casos, los hackers utilizan cuentas auténticas pero desvían la información. Cualesquiera peticiones no solicitadas que impliquen una transacción financiera deben gestionarse con extrema precaución.
- Asegurarse de que su **antivirus** está actualizado con la última versión.
- Consultar con sus bancos sobre actualizaciones para que su **software de pago en línea** sea más seguro.
- Solicitar **diligencia debida adicional si la cuenta bancaria** de un proveedor o un receptor no coincide con la ubicación del proveedor o se ha producido un cambio en el país donde la cuenta bancaria está registrada. Puede solicitar una carta del proveedor o el receptor debidamente firmada para confirmar la autenticidad de la cuenta bancaria.
- Solicitar confirmación adicional mediante una llamada telefónica.
- Crear verificaciones integrales adicionales para los pagos realizados a cuentas bancarias nuevas.
- Trabajar con sus departamentos de TI para disponer de formaciones de actualización destinadas al personal con el fin de mejorar la sensibilización sobre estas cuestiones En particular enfocar la formación en la dirección del MCP, el personal de la Secretaría del MCP y el personal del RP sobre correos electrónicos fraudulentos.