El Fondo Mundial

NOTA ORIENTATIVA SOBRE SISTEMAS DE INFORMACIÓN E INTERCAMBIO DE DATOS

19 de agosto de 2020

Objetivo

La utilización de sistemas de información, entre ellos las comunicaciones por correo electrónico y el intercambio de datos electrónicos, es fundamental para el logro efectivo de los objetivos de la organización y es clave para la disponibilidad eficiente, fiable y oportuna de datos financieros que permitan adoptar decisiones a diversos niveles en el ámbito de ejecución de la subvención.

Sin embargo, la utilización de los sistemas de información expone a las organizaciones a riesgos de ciberseguridad, entre ellos los mensajes de correo de suplantación de identidad (*phishing*), práctica fraudulenta que se utiliza para recopilar información importante de los usuarios o proporcionarles información incorrecta con el fin de obtener ventajas ilícitas.

En consecuencia, se espera que los receptores principales actualicen, según sea necesario, su manual interno de procedimientos y directrices para asegurar que se establezcan controles de gestión eficaces a fin de salvaguardar los datos relacionados con las actividades ejecutadas mediante subvenciones del Fondo Mundial. En concreto, se deben proteger los datos esenciales, especialmente los relativos a cuentas bancarias, proveedores, suministradores de servicios, consultores y personal. Ello puede requerir la introducción o modificación de procedimientos para aplicar esos controles, como se indica en las recomendaciones que figuran a continuación.

La presente nota orientativa no modifica ningún derecho ni obligación en virtud de los acuerdos de subvención del Fondo Mundial, ni constituye una renuncia a ellos. Los receptores principales deben seguir asegurándose de que ellos y todos sus asociados ejecutores de programas (incluidos los subreceptores, proveedores y contratistas) cumplen las leyes y reglamentos aplicables, como los relativos a la recopilación y el procesamiento de datos personales y a la transferencia de esos datos al Fondo Mundial cuando se soliciten[1].

Principios clave

Los siguientes principios clave deben aplicarse en todos los casos, independientemente del tipo de datos esenciales de que se trate:

- **Separación de responsabilidades**. El personal encargado de tramitar los pagos no podrá a acceder a la base de datos maestra conexa mantenida por el Receptor Principal o el asociado ejecutor de programas, ni efectuar cambios en ella. Cualquier cambio en los datos esenciales deberá ser aprobado por un miembro del personal de categoría superior que cuente con la

[1] Para más información, consulte las declaraciones de privacidad del Fondo Mundial en https://www.theglobalfund.org/en/legal/privacy-statement/

debida autoridad y que desempeñe funciones distintas a las de las personas que llevan a cabo los procesos de pago y modificación.

- **Rendición de cuentas**. La base de datos debe ser gestionada por personal que cuente con la debida autoridad sobre cada módulo respectivo y debe existir una integración entre los módulos. El principio se aplica a la gestión de los archivos de Excel en caso de que se utilice un sistema de entrada de datos manual.
- **Confirmación**. Con respecto a todos los pagos superiores a US$ 50.000[2], se recomienda encarecidamente que, antes de iniciar el pago, el Receptor Principal obtenga una confirmación oficial de la persona de contacto designada por el proveedor.

Controles específicos

1. Cuentas bancarias

- Los datos relativos a cuentas bancarias deben ser mantenidos en el módulo de gestión de efectivo de la base de datos, o en archivos en el caso de un sistema manual, por una persona o departamento que desempeñe funciones distintas a las de la persona o el departamento responsable de la tramitación de los pagos.
- Se alienta encarecidamente a los receptores principales a que apliquen requisitos de firma múltiple para las transacciones materiales y/o complejas. También se los alienta a que procedan a la rotación periódica de los signatarios autorizados de los desembolsos.
- Los requisitos (que figuran en el anexo 1) relativos a la adición o eliminación de información de cuentas bancarias deben cumplirse antes de actualizar el módulo de gestión de efectivo de la base de datos, o los sistemas manuales, según proceda. Para obtener más información, consulte la Sección 5.6.1 – *Bank Account Management* de la publicación Financial Management Handbook for Grant Implementers.

2. Proveedores y suministradores de servicios

- Los receptores principales deben contar con un proceso claro para realizar comprobaciones de antecedentes y de diligencia debida antes de firmar o modificar un contrato con cualquier proveedor o suministrador de servicios, incluida la verificación de información clave como el registro de empresas (mediante certificados) y los datos de cuentas bancarias.
- Toda la información clave, incluido el nombre de la organización, el signatario autorizado, la persona de contacto, el domicilio social y los detalles de la cuenta bancaria, debe incluirse expresamente en el contrato.
- Toda solicitud de modificación de la información clave del proveedor o del suministrador de servicios deberá estar respaldada por la documentación apropiada y haber sido verificada y aprobada por el personal autorizado antes de que dicha modificación pueda hacerse efectiva en la base de datos y el contrato.
- La correspondencia confidencial, incluida la relativa a cualquier solicitud de cambio de información clave del proveedor o suministrador de servicios, debe realizarse únicamente por conducto de la persona de contacto designada en el contrato.
- El proveedor o suministrador de servicios debe clasificarse como inactivo en el sistema solo cuando se hayan cumplido plenamente todas las responsabilidades y obligaciones previstas en cualquier contrato en el que participe dicho proveedor o suministrador de servicios.

[2] O bien el umbral definido por el Receptor Principal, si es más bajo.

3. **Personal y consultores**
   - Los datos personales, incluidos los nombres, las fechas de nacimiento y los detalles de las cuentas bancarias, deben ser mantenidos en el módulo Recursos Humanos (RRHH) de la base de datos, o en los archivos de los empleados, por personal autorizado del Receptor Principal.
   - El personal encargado de la preparación de las nóminas y/o los pagos no podrá tener derechos ni acceso para modificar o cambiar los datos personales de los empleados de la organización.
   - Para facilitar los procesos de pagos, los datos personales del módulo de recursos humanos deben integrarse con los datos del módulo de gestión de efectivo. En el caso de un sistema manual, deben existir controles de gestión adecuados, que incluyan la verificación, la revisión y la aprobación.
   - Para obtener más información sobre la creación, modificación o supresión de datos del personal, consulte la Sección 4.5 - *Human Resources* de la publicación "Financial Management Handbook for Grant Implementers".
   - Deberían establecerse salvaguardias para los datos que identifican, o podrían utilizarse para identificar, a personas, como por ejemplo miembros del personal y consultores. Las salvaguardias pueden incluir medidas técnicas y organizativas, como permisos de acceso, anonimización, clasificación confidencial de datos personales delicados, períodos de retención para garantizar que los datos personales no se mantengan más tiempo del necesario y sistemas seguros de almacenamiento y transferencia de datos personales.
   - Para obtener más orientación sobre la protección de los datos personales, sírvase consultar las recomendaciones formuladas por la autoridad de protección de datos competente de su jurisdicción.

Fortalecimiento de los sistemas de gestión de la seguridad de la información

Las entidades ejecutoras deberían tomar medidas para reforzar continuamente la seguridad de la información de su arquitectura digital y de tecnologías de la información, siguiendo las normas internacionales de mejores prácticas, como la ISO 27001[3] y la ISO 27002 (códigos de prácticas)[4]. Estas normas marco proporcionan a las entidades ejecutoras orientación sobre la forma de gestionar los riesgos para la seguridad de la información, con miras a preservar la confidencialidad, la integridad y la disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y asegurando a las partes interesadas que los riesgos se gestionan adecuadamente.

Además, las siguientes referencias pueden ayudar a las entidades ejecutoras a desarrollar sus arquitecturas digitales y de tecnología de la información, en particular a definir políticas y normas de seguridad y protección de la privacidad:

1. Conjunto de herramientas de la OMS y la UIT sobre estrategias nacionales de cibersalud[5];
2. Digital Health Platform Handbook: Building a Digital Information Infrastructure (infrastructure) for Health. Ginebra: Unión Internacional de Telecomunicaciones[6];y
3. Principles for Digital Development[7].

[3] https://www.iso.org/isoiec-27001-information-security.html

[4] https://www.iso.org/standard/54533.html

[5] https://apps.who.int/iris/bitstream/handle/10665/75211/9789241548465_eng.pdf?sequence=1&isAllowed=y

[6] https://ehna.acfee.org/c67802a7d4b3dc8914700842bf6776402b8d343c.pdf

[7] https://digitalprinciples.org/

Formación del personal

Como parte de la gestión básica de los riesgos financieros y la ciberseguridad y de las buenas prácticas, los receptores principales deben asegurarse de que el personal posea la formación adecuada y conozca las características y los métodos que se emplean en los ataques contra la ciberseguridad, incluido el *phishing*. Debe disponerse de personal especializado para recibir y atender las consultas relacionadas con los riesgos financieros y en materia de ciberseguridad.

Existe un curso de formación en línea sobre phishing para asociados externos (enlace). Todo el personal de MCP, RP y SR que participe en transacciones financieras debe seguir esta formación. Su duración es de 15 minutos.

Todo el personal que participe en las siguientes actividades deberá seguir la formación:

1. Modificación de datos de terceros (bancos, proveedores, personal y consultores);
2. Pago de transacciones; y
3. Ordenación de pagos.

Los RP también son responsables de asegurar que los SR completen la formación. Los agentes locales del Fondo verificarán la ejecución de la formación durante la próxima revisión del PU/DR.

Los participantes que no estén inscritos en la plataforma iLearn del Fondo Mundial deberán dedicar unos minutos a inscribirse (aquí). Una vez inscritos, podrán acceder a otros cursos gratuitos del Fondo Mundial de aprendizaje electrónico, como los dedicados a la elaboración de subvenciones y la presentación de informes de RP.

En el anexo 2 de la presente nota orientativa se destacan las opciones y los recursos conexos. Los receptores principales deberán explorar estos y otros recursos disponibles y asegurarse de que se alienta firmemente al personal a que adquiera la debida formación.

Anexo 1: Recomendaciones acerca de los procedimientos internos para la creación, modificación o supresión de datos clave relacionados con proveedores y suministradores de servicios.

Información clave	Creación	Modificación	Supresión
Cuenta bancaria	▪ Los detalles de la cuenta bancaria deben incluirse en la base de datos solo cuando: ✓ Se proporcione un formulario de información bancaria (preferiblemente en un formato predefinido suministrado por el RP); ✓ El proveedor o suministrador de servicios proporcione una lista de signatarios autorizados de cuentas bancarias (por lo menos dos signatarios), con muestras de firmas certificadas; ✓ Se proporcionen procedimientos que permitan la firma múltiple para transacciones complejas o de gran envergadura (por encima de un umbral definido); ✓ Se obtenga una confirmación formal (carta) del banco titular de la cuenta, en papel con membrete del banco; ✓ El banco titular de la cuenta esté incluido en la lista del Banco Mundial de bancos comerciales elegibles (u otra lista reconocida internacionalmente); ✓ Se haya acreditado al banco después de haberlo sometido a sistemas de detección antiterrorista, por ejemplo, mediante ✓ https://bridgerinsight.lexisnexis.com/; ✓ Se haya verificado el IBAN de la cuenta, por ejemplo mediante https://www.tbg5-finance.org/?ibancheck.shtml; y ✓ Se haya verificado el código SWIFT del banco mediante https://www2.swift.com/bsl/index.faces ➢ **Señales de alarma**: ○ La cuenta bancaria figura bajo un nombre distinto al del proveedor o el suministrador de servicios. ○ La dirección del titular de la cuenta es diferente del domicilio fiscal del proveedor o del suministrador de servicios	▪ Los detalles de la cuenta bancaria deberán modificarse solo cuando: ✓ Se sigan todos los pasos descritos en la columna Creación. ✓ La solicitud sea enviada por la persona de contacto designada mediante una comunicación formal en papel con membrete oficial; ✓ La solicitud haya sido debidamente firmada por un signatario autorizado; ✓ La solicitud incluya una justificación válida para la modificación; ✓ La modificación deba ser revisada por personal superior antes de que sea validada; y ✓ La persona que tramite el pago no sea la que valide la modificación (separación de funciones)	▪ Los detalles de la cuenta bancaria deben clasificarse como inactivos en la base de datos cuando se hayan cumplido íntegramente todas las obligaciones derivadas de cualquier contrato pertinente. ▪ El personal superior independiente debe revisar anualmente la totalidad de la base de datos de proveedores y suministradores de servicios para confirmar si están activos o inactivos. ➢ **Señales de alarma**: no quedan obligaciones pendientes en virtud de ningún contrato pertinente, pero el proveedor o el suministrador de servicios sigue figurando como activo en la base de datos.
Contacto para notificaciones	La información de contacto (incluida la dirección de correo electrónico) de la persona autorizada para recibir y enviar correspondencia en nombre del proveedor o suministrador de servicios debe incluirse en cada contrato pertinente.	Se deben seguir todos los pasos descritos en la columna Creación. Toda solicitud de modificación de la información de la persona de contacto deberá ser presentada únicamente por un representante autorizado de la entidad mediante una carta oficial corroborada por las entidades ejecutoras (por el personal superior de las entidades	

Información clave	Creación	Modificación	Supresión
		ejecutoras y/o la entidad interesada para la que trabaje la persona en cuestión).	
Signatario del contrato autorizado	La información de los signatarios autorizados deberá especificarse solo cuando: ✓ Se presente y verifique una prueba de la autoridad para firmar el contrato pertinente en nombre de la entidad (por ejemplo, el certificado del personal directivo superior; los estatutos); y ✓ El signatario proporcione una muestra certificada de su firma (preferiblemente en un formato predefinido suministrado por el RP o la entidad ejecutora de la subvención).	Se deben seguir todos los pasos descritos en la columna Creación. Toda solicitud de modificación de los signatarios autorizados (por ejemplo, para introducir modificaciones en el contrato) debe ser enviada por la persona de contacto designada mediante una comunicación formal en papel con membrete oficial debidamente verificada por la entidad ejecutora mediante la confirmación del personal directivo superior antes de efectuar cualquier modificación.	
Dirección de la otra parte y detalles de contacto	El domicilio social, la dirección postal, el correo electrónico, el fax y el número de teléfono de la entidad deben figurar en cada contrato pertinente. El domicilio social debe verificarse mediante la consulta de registros públicos en el caso de que existan.	Toda solicitud de modificación del domicilio social o de la dirección postal de la entidad deberá ser presentada por la persona de contacto de la entidad, debidamente verificada por la entidad ejecutora mediante la confirmación del personal directivo superior antes de efectuar cualquier modificación. Se deben seguir todos los pasos descritos en la columna “Creación”.	

Anexo 2: Recursos adicionales de seguridad de la información para hacer frente a los riesgos de ciberseguridad

Además del curso de formación en línea sobre phishing que ofrece el Fondo Mundial, los receptores principales pueden solicitar una serie de servicios de seguridad de la información a los proveedores pertinentes:

1. Formación en materia de sensibilización sobre la seguridad de la información
2. Fortalecimiento de los sistemas de gestión de información

El Fondo Mundial está ultimando una lista de proveedores de asistencia técnica previamente aprobados para ayudar a los RP y otras entidades ejecutoras de subvención a mejorar los sistemas de gestión de la información y la ciberseguridad.

Además, los receptores principales y otras entidades ejecutoras de subvención pueden considerar la posibilidad de recurrir a la autenticación multifactorial. Para activar este tipo de autenticación, consulte los términos y condiciones y la orientación del suministrador de servicios de correo electrónico correspondiente. A continuación, se presenta más información al respecto sobre Gmail y Yahoo.

- Gmail : https://www.google.com/landing/2step/
- Yahoo: https://help.yahoo.com/kb/add-two-step-verification-extra-security-sln5013.html

Es recomendable que los receptores principales y otras entidades ejecutoras de subvención también consulten el código de prácticas de la ISO 27002 relativo a los controles de la seguridad de la información[8]. Un sistema sólido de gestión de la seguridad de la información puede beneficiar a los receptores principales y a otras entidades ejecutoras de subvención al brindar a sus beneficiarios y las partes interesadas la confianza de que pueden proteger su información, gestionar sus finanzas y mejorar la seguridad de la cadena de suministro.

[8] https://www.iso.org/standard/54533.html