O Fundo Global

NOTA DE ORIENTAÇÃO SOBRE SISTEMAS DE INFORMAÇÃO E PARTILHA DE DADOS

19 de agosto de 2020

Objetivo

A utilização de sistemas de informação, incluindo as comunicações por e-mail e a partilha de dados eletrónicos, é fundamental para alcançar eficazmente os objetivos da organização e um elemento-chave para a disponibilidade eficiente, fiável e atempada de dados financeiros para a tomada de decisões a vários níveis da execução da subvenção.

No entanto, a utilização de sistemas de informação expõe as organizações a riscos de cibersegurança, incluindo e-mails de *phishing*, uma prática fraudulenta utilizada para recolher informações importantes dos utilizadores ou proporcionar-lhes informações incorretas com o intuito de obter vantagens ilegais.

Em conformidade, espera-se que os Beneficiários Principais atualizem, conforme necessário, o seu manual de procedimentos interno e diretrizes para assegurar a existência de controlos de gestão eficazes a fim de salvaguardar os dados relacionados com as atividades implementadas através das subvenções do Fundo Global. Em especial, os dados críticos devem estar em segurança, particularmente os dados relacionados com contas bancárias, fornecedores, prestadores de serviços, consultores e funcionários. Poderá ser necessário introduzir ou alterar procedimentos para implementar estes controlos, conforme descrito nas recomendações abaixo.

Esta nota de orientação não emenda nem constitui uma renúncia de quaisquer direitos ou obrigações ao abrigo dos acordos de subvenção do Fundo Global. Os Beneficiários Principais, assim como todos os seus parceiros implementadores (incluindo os Beneficiários Secundários, fornecedores e adjudicatários), devem continuar a assegurar que cumprem as leis e regulamentações aplicáveis, como as que estão relacionadas com a recolha e o tratamento de dados pessoais e a transferência dos mesmos para o Fundo Global a pedido[1].

Princípios fundamentais

Os seguintes princípios fundamentais devem ser aplicados em todos os casos, independentemente da natureza dos dados críticos:

- **Separação de responsabilidades.** Os funcionários responsáveis por processar os pagamentos não devem ter o direito de aceder ou efetuar alterações à base de dados principal associada, mantida pelo Beneficiário Principal ou implementador da subvenção. As alterações

[1] Para mais informações, consulte as Declarações de privacidade do Fundo Global https://www.theglobalfund.org/en/legal/privacy-statement/

aos dados críticos devem ser aprovadas por um funcionário de nível superior devidamente autorizado, funcionalmente separado das pessoas que tratam dos processos de pagamento e correção.

- **Responsabilização**. A base de dados deve ser gerida pelos funcionários que detêm a devida autoridade sobre os respetivos módulos e deve haver integração entre os módulos. O princípio aplica-se à gestão de ficheiros Excel se o sistema for de introdução manual.
- **Confirmação**. Para todos os pagamentos acima de 50 000 dólares[2], é vivamente recomendado que o Beneficiário Principal obtenha a confirmação formal da pessoa de contacto designada pelo fornecedor antes de iniciar o pagamento.

Controlos específicos

1. **Contas bancárias**
   - Os dados relacionados com contas bancárias devem ser mantidos no módulo Gestão de Caixa da base de dados ou nos ficheiros, caso se trate de um sistema manual, por uma pessoa ou departamento funcionalmente separado da pessoa ou departamento responsável por processar os pagamentos.
   - Os Beneficiários Principais são vivamente encorajados a implementar requisitos que exijam vários signatários para transações importantes e/ou complexas. Os Beneficiários Principais são também encorajados a alterar regularmente os signatários autorizados para realizar desembolsos.
   - É necessário seguir os requisitos (conforme descritos no Anexo 1) relacionados com a adição ou eliminação de informações de contas bancárias antes de atualizar o módulo Gestão de Caixa da base de dados ou os sistemas manuais, conforme apropriado. Consulte a secção 5.6.1 – *Gestão de Contas Bancárias* do Manual de Gestão Financeira para Implementadores de subvenções para mais informações.

2. **Fornecedores e prestadores de serviços**
   - Os Beneficiários Principais devem ter um processo claro para a realização de verificações de antecedentes e de *due diligence* antes de assinar ou alterar um contrato com qualquer fornecedor ou prestador de serviços, incluindo a verificação de informações fundamentais, como o registo de empresas (através de certificados) e dados de contas bancárias.
   - Todas as informações-chave, incluindo o nome da organização, signatário autorizado, pessoa de contacto, endereço registado e dados da conta bancária, devem ser expressamente incluídas no contrato.
   - Qualquer pedido para alterar quaisquer informações-chave do fornecedor ou prestador de serviços deve ser justificado por documentação adequada, verificada e aprovada por pessoal autorizado antes de as informações poderem ser alteradas na base de dados e no contrato.
   - A correspondência confidencial, incluindo a relacionada com qualquer pedido para alterar as informações-chave do fornecedor ou prestador de serviços, deve ser realizada somente através da pessoa de contacto designada no contrato.
   - O fornecedor ou prestador de serviços deve ser classificado como inativo no sistema somente quando todas as responsabilidades e obrigações ao abrigo de qualquer contrato envolvendo o fornecedor ou prestador de serviços tenham sido integralmente cumpridas.

[2] Ou o limite definido pelo Beneficiário Principal, caso seja inferior.

3. **Funcionários e consultores**
   - Os dados pessoais, incluindo nomes, datas de nascimento e dados de contas bancárias, devem ser mantidos no módulo Recursos Humanos (RH) da base de dados, ou nos ficheiros do pessoal, por funcionários autorizados do Beneficiário Principal.
   - Os funcionários responsáveis pela preparação das folhas de salários e/ou dos pagamentos não devem ter direitos ou acesso para modificar ou alterar os dados pessoais dos funcionários da organização.
   - Os dados pessoais no módulo de RH devem ser integrados nos dados do módulo de gestão de caixa para facilitar os processos de pagamento. Caso se trate de um sistema manual, devem estar implementados controlos de gestão adequados, incluindo verificação, análise e aprovação.
   - Para mais informações sobre a criação, modificação ou eliminação de dados dos funcionários, consulte a Secção 4.5 – *Recursos Humanos* do "Manual de Gestão Financeira para Implementadores de Subvenções".
   - Devem existir salvaguardas para dados que identifiquem, ou que possam ser utilizados para identificar, indivíduos como funcionários e consultores. As salvaguardas podem incluir medidas técnicas e organizacionais como permissões de acesso, transformação em forma anónima, classificação confidencial de dados pessoais sensíveis, períodos de retenção para assegurar que os dados pessoais não sejam mantidos mais tempo do que o necessário e sistemas seguros para conservar e transferir dados pessoais.
   - Para mais orientações sobre proteção de dados pessoais, consulte as recomendações emitidas pela autoridade de proteção de dados aplicável na sua jurisdição.

Reforce os seus sistemas de gestão de segurança da informação

Os implementadores devem tomar medidas para reforçar continuamente a segurança da informação da sua arquitetura digital e de tecnologia de informação, obedecendo às normas internacionais de melhores práticas, como, por exemplo, a ISO 27001[3] e a ISO 27002 (códigos de conduta)[4]. Estas normas de enquadramento oferecem aos implementadores orientações sobre a forma de gerir os riscos de segurança da informação, com vista a preservar a confidencialidade, integridade e disponibilidade da informação através da aplicação de um processo de gestão de riscos e a garantir às partes interessadas que os riscos são geridos adequadamente.

Além disso, as seguintes referências podem ajudar os implementadores no desenvolvimento das respetivas arquiteturas digital e de tecnologia de informação, incluindo a definição de políticas e normas de segurança e proteção da privacidade:

1. Kit de Ferramentas da Estratégia Nacional de Saúde Eletrónica da OMS UIT[5];
2. Manual da Plataforma de Saúde Digital: Construir uma Infraestrutura de Informação Digital (infraestrutura) para a Saúde. Genebra: União Internacional das Telecomunicações[6]; e
3. Princípios do Desenvolvimento Digital[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/

Formação do pessoal

Enquanto parte da gestão e boas práticas básicas em matéria de riscos financeiros e de cibersegurança, espera-se que os Beneficiários Principais garantam que o pessoal recebe a devida formação e esteja ciente dos métodos e caraterísticas utilizados nos ataques de cibersegurança, incluindo o *phishing*. Deve haver pessoal dedicado à receção e resposta a dúvidas relacionadas com riscos financeiros e de cibersegurança.

Está disponível aos parceiros externos um Curso de Formação sobre Phishing online (ligação). Todos os funcionários do MCP, BP e BS envolvidos em transações financeiras devem realizar esta formação. A ação de formação tem a duração de 15 minutos.

Os funcionários envolvidos nas seguintes atividades devem realizar a ação de formação:

1. Modificação de dados de terceiros (bancos, fornecedores, funcionários e consultores);
2. Pagamento de transações; e
3. Emissão de ordens de pagamento.

Os BP são também responsáveis por assegurar que os BS realizem a ação de formação. Os Agentes Locais do Fundo irão verificar a implementação da ação de formação durante a análise seguinte do RP/PD.

Os participantes que não estejam registados na plataforma iLearn do Fundo Global devem reservar alguns minutos para se registarem (aqui). Depois de registados, poderão aceder a outros cursos de e-Learning gratuitos do Fundo Global, como a Elaboração da Subvenção e os Relatórios do BP.

O Anexo 2 desta nota de orientação destaca opções e recursos relacionados com os referidos cursos. Os Beneficiários Principais devem explorar estes e outros recursos disponíveis e garantir que os funcionários sejam vivamente encorajados a realizar a formação adequada.

Anexo 1: Recomendações sobre procedimentos internos para a criação, alteração ou eliminação de dados-chave relacionados com fornecedores e prestadores de serviços.

Informações-chave	Criação	Alteração	Eliminação
Conta bancária	▪ Os dados da conta bancária devem ser incluídos na base de dados somente quando: ✓ For fornecido um formulário de informação do banco (preferencialmente num formato predefinido fornecido pelo BP); ✓ For fornecida uma lista de signatários da conta bancária autorizados (pelo menos dois signatários), com exemplares da assinatura certificados, pelo fornecedor ou prestador de serviços; ✓ Forem indicados procedimentos relativos a múltiplas assinaturas para transações complexas ou de grande dimensão (acima de um limiar definido); ✓ For obtida uma confirmação formal (carta) junto do banco que detém a conta, em papel timbrado do banco; ✓ O banco que detém a conta estiver incluído na lista de bancos comerciais elegíveis do Banco Mundial (ou outra lista internacionalmente reconhecida); ✓ O banco tiver sido aprovado na sequência de controlos antiterroristas, como, por exemplo, através de ✓ https://bridgerinsight.lexisnexis.com/; ✓ O IBAN da conta tiver sido verificado, como, por exemplo, através de https://www.tbg5-finance.org/?ibancheck.shtml; e ✓ O código SWIFT da conta for verificado através de https://www2.swift.com/bsl/index.faces ➢ **Sinais de alerta:** ○ A conta bancária está num nome diferente do nome do fornecedor ou prestador de serviços ○ O endereço do titular da conta é diferente do endereço registado do fornecedor ou prestador de serviços	▪ Os dados da conta bancária devem ser alterados somente quando: ✓ Todos os passos descritos na coluna criação tiverem sido seguidos; ✓ O pedido for enviado pela pessoa de contacto designada através de uma comunicação formal em papel timbrado oficial; ✓ O pedido for devidamente assinado por um signatário autorizado; ✓ O pedido incluir uma justificação válida para a alteração; ✓ A alteração deve ser analisada por um funcionário de nível superior antes de ser validada; e ✓ A pessoa que processa o pagamento não for a pessoa que valida a alteração (separação de deveres)	▪ Os dados da conta bancária devem ser classificados como inativos na base de dados quando todos as responsabilidades relativas a qualquer contrato relevante tiverem sido integralmente cumpridas. ▪ Funcionários independentes de nível superior devem analisar toda a base de dados do fornecedor/prestador de serviços anualmente para confirmar o estado ativo e inativo. ➢ **Sinais de alerta**: Não existem responsabilidades pendentes no âmbito de nenhum contrato relevante, mas o fornecedor ou prestador de serviços ainda está classificado como ativo na base de dados.
Contacto para notificações	Os dados de contacto (incluindo o endereço de e-mail) da pessoa autorizada a receber e enviar correspondência em nome do fornecedor ou prestador de serviços devem estar incluídos em cada contrato relevante.	Todos os passos descritos na coluna criação devem ser seguidos. Qualquer pedido de alteração dos dados da pessoa de contacto deve ser comunicado somente por um representante autorizado da entidade através de uma carta formal, confirmado mais uma vez pelos implementadores (pelos funcionários de nível superior dos implementadores e/ou pela entidade relevante para a qual a pessoa trabalha).	

Informações-chave	Criação	Alteração	Eliminação
Signatário do contrato autorizado	Os dados do signatário autorizado devem ser criados somente quando: ✓ For fornecida e verificada uma prova de autorização para assinar o contrato relevante em nome da entidade (por exemplo, certificado da gestão de topo; estatutos); e ✓ O signatário fornecer um exemplar da assinatura certificado (preferencialmente num formato predefinido fornecido pelo BP ou implementador da subvenção).	Todos os passos descritos na coluna criação devem ser seguidos. Qualquer pedido para alterar os signatários autorizados (por exemplo, para emendas ao contrato) deve ser enviado pela pessoa de contacto designada através de uma comunicação oficial em papel timbrado oficial devidamente verificada pelo implementador através da confirmação da gestão de topo antes de efetuar qualquer alteração.	
Endereço e dados de contacto da contraparte	O endereço registado, endereço postal, endereço de e-mail, fax e número de telefone da entidade devem ser incluídos em cada contrato relevante. O endereço registado deve ser verificado através de registos públicos quando disponíveis.	Qualquer pedido para alterar o endereço registado ou postal deve ser comunicado pela pessoa de contacto da entidade devidamente verificada pelo implementador através de confirmação da gestão de topo antes de efetuar qualquer alteração. Todos os passos descritos na coluna “Criação” devem ser seguidos.	

Anexo 2: Recursos de segurança da informação adicionais para abordar riscos de cibersegurança

Além do curso online de Formação sobre Phishing fornecido pelo Fundo Global, os Beneficiários Principais podem solicitar uma série de serviços de segurança da informação aos prestadores de serviços de segurança da informação:

1. Formação sobre consciencialização da segurança da informação
2. Reforço dos sistemas de gestão da informação

O Fundo Global está a finalizar uma lista de fornecedores de assistência técnica pré-aprovados para ajudar os BP e outros implementadores das subvenções a melhorar os sistemas de gestão da informação e a cibersegurança.

Além disso, os Beneficiários Principais e outros implementadores das subvenções poderão ponderar utilizar a autenticação multifator. Consulte os termos e condições do prestador do serviço de e-mail relevante e respetivas orientações para ativar a autenticação multifator. Veja abaixo mais dados relativos ao Gmail e ao Yahoo.

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

Os Beneficiários Principais e outros implementadores das subvenções poderão também querer consultar a norma ISO 27002, que estabelece o código das melhores práticas em controlos de segurança da informação[8]. Um sistema de gestão da segurança da informação robusto pode beneficiar os Beneficiários Principais e outros implementadores das subvenções ao proporcionar aos seus beneficiários e partes interessadas a confiança necessária para poderem proteger as suas informações, gerir as suas finanças e melhorar a segurança da cadeia de abastecimento.

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