Folha de conselhos sobre a segurança dos dados na gestão dos dados operacionais
Abril de 2022

A tradução desta folha de conselhos foi facilitada pela CartONG graças ao apoio da CLEAR Global e do Ministério Francês da Europa e dos Negócios Estrangeiros.

Introdução
A segurança dos dados é um componente fundamental da responsabilização dos dados: a gestão segura, ética e eficaz dos dados para a resposta operacional. Implica um conjunto de medidas físicas, tecnológicas e processuais que salvaguardam a confidencialidade, a integridade e a disponibilidade dos dados e evitam a sua perda, destruição, alteração, aquisição ou divulgação acidental ou intencional, ilegal ou não autorizada.

Esta folha de conselhos oferece um conjunto de ações recomendadas para a segurança dos dados na sua gestão operacional. As ações devem ser implementadas em conformidade com os mandatos institucionais, as políticas e os quadros jurídicos e regulamentares relevantes.

Pratique uma boa gestão das palavras-passe
- Proteja os seus dispositivos e as suas contas com palavras-passe fortes com, pelo menos, 16 caracteres, que incluem números, letras maiúsculas e minúsculas e símbolos.
- Ative a autenticação multifator para todas as contas.
- Não reutilize a mesma palavra-passe para várias contas.
- Não armazene as suas palavras-passe fisicamente (por exemplo, em blocos de nota) ou digitalmente (num arquivo no seu dispositivo) e não partilhe a sua palavra-passe com outras pessoas.
- Não ative a funcionalidade 'Lembrar-me' nas aplicações ou nos navegadores.
- Modifique imediatamente as suas palavras-passe nas suas contas online se o seu dispositivo for perdido ou roubado.

Utilize um programa antivírus/antimalware
- Certifique-se de ter um programa antivírus/antimalware apropriado nos seus dispositivos.
- Se tiver dúvidas sobre as ferramentas apropriadas ou como configurá-las, consulte o especialista de TI do seu escritório.

Mantenha os programas e os sistemas operacionais atualizados
- Verifique regularmente que o seu dispositivo, os seus programas, as suas aplicações e os plug-ins do navegador estão atualizados e ativam as atualizações automáticas do seu sistema operacional.
- Utilize navegadores como o Chrome ou o Firefox que recebem atualizações de segurança automáticas.
- Desligue os dispositivos ao final do dia para permitir a atualização e proteger-se contra ataques.

Evite os esquemas de *phishing* e seja prudente com o elemento no qual clica
- Ao receber e-mails ou mensagens suspeitas, verifique sempre o endereço e as informações de contacto do remetente e clique apenas nas ligações ou nos anexos quando confiar no remetente.
- Não responda a e-mails suspeitos nem os encaminhe aos seus colegas.
- Denuncie qualquer atividade suspeita à sua equipa de suporte de TI.

Utilize os dispositivos móveis com responsabilidade

- **Sempre que possível, utilize dispositivos separados para o seu trabalho. Mantenha sempre os seus dispositivos de trabalho num local seguro e evite transportá-los desnecessariamente.**
- **Utilize ferramentas de mensagens aprovadas pela sua empresa e que forneçam uma encriptação de ponta a ponta.**
- **Desligue a conectividade Bluetooth quando possível e minimize-a.**
- **Utilize uma Rede Privada Virtual (VPN) aprovada pela sua empresa ao trabalhar online. Desligue sempre a(s) sua(s) conta(s) ao utilizar um computador ou um dispositivo comunitário.**
- **Desative os recursos de desbloqueio biométrico, principalmente quando estiver em trânsito.**

Proteja os dados confidenciais e pratique a minimização dos dados

- **Mantenha um registo dos ativos dos dados que indique o nível de confidencialidade de cada tipo de dados geridos pelo seu escritório. Analise os níveis de confidencialidade regularmente à medida que o contexto evolui.**
- **Recolhe apenas a quantidade mínima de dados necessária para atingir o objetivo e as finalidades de uma determinada atividade de gestão dos dados.**
- **Retenha os dados confidenciais apenas durante o tempo necessário para atingir o objetivo para o qual estão geridos e conforme exigido pelas orientações, as leis e os regulamentos aplicáveis.**
- **Transfira e armazene os dados utilizando ferramentas e canais aprovados pela sua empresa (localmente num servidor, num computador ou num portátil da empresa; ou em servidores e sistemas operados remotamente por meio de aplicações como OneDrive, SharePoint e Teams).**
- **Proteja com senha os ficheiros (Word, Excel, PDF) contendo dados confidenciais e partilhe as senhas dos documentos por meio de canais separados (ou seja, envie uma senha por SMS para um documento enviado por e-mail).**
- **Limite e monitorize cuidadosamente o número de pessoas com acesso aos dados confidenciais.**
- Defina um calendário de retenção e de destruição de todos os dados geridos e utilize ferramentas adequadas para a destruição dos dados.
- Codifique os seus e-mails.

Principais recursos

- Orientações Operacionais do IASC sobre a Responsabilidade dos Dados na Ação Humanitária
- Nota de orientação sobre a gestão dos incidentes ligados aos dados
- Folha de conselhos sobre a utilização responsável das ferramentas de conferência online

Para obter mais informações sobre a gestão dos dados confidenciais nas operações humanitárias, visite a página Responsabilidade dos Dados no website do Centro ou contacte a nossa equipa em centrehumdata@un.org.