ESCOLA de CIÊNCIA da INFORMAÇÃO
UFMG

75 ANOS
1950-2025

MANUAL DE CIBERSEGURANÇA E PRIVACIDADE DE DADOS PARA GLAM

Museus, Bibliotecas, Arquivos e Galerias

Ana Cecília Rocha Veiga

2026

MANUAL

DE CIBERSEGURANÇA E PRIVACIDADE DE DADOS PARA GLAM

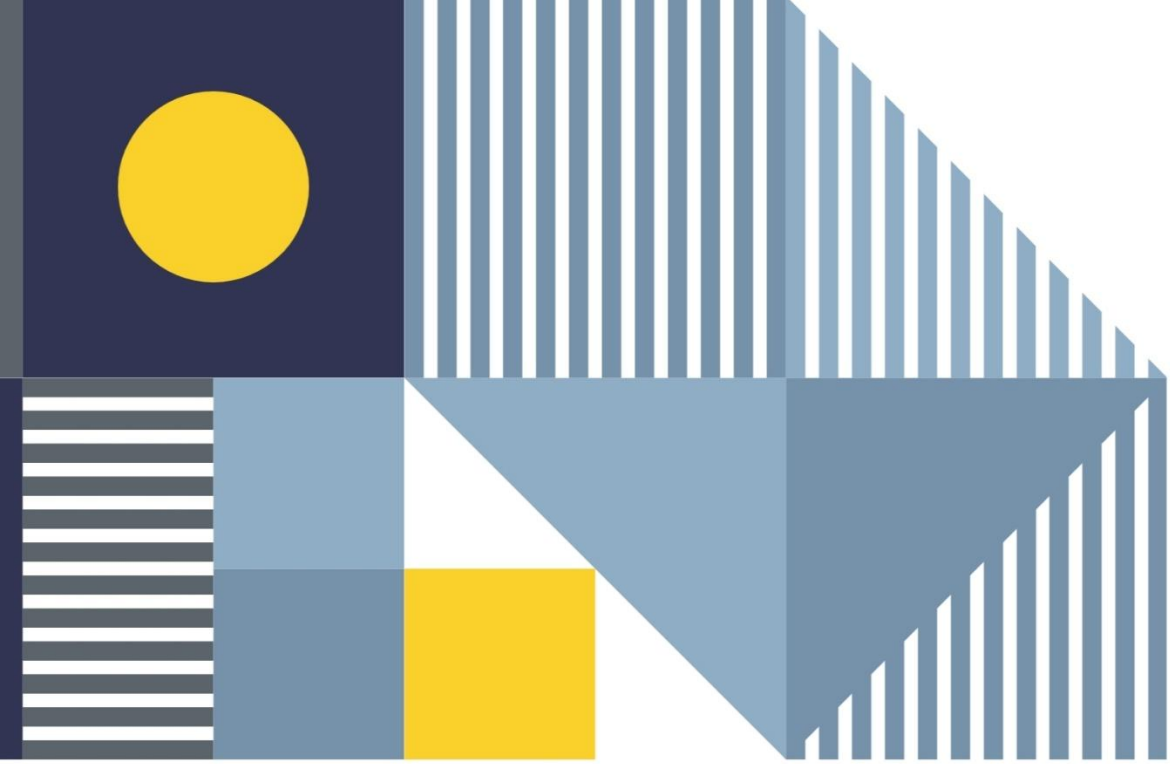
MUSEUS, BIBLIOTECAS, ARQUIVOS E GALERIAS

VERSÃO 1.0 - MARÇO DE 2026

ESCOLA de CIÊNCIA da INFORMAÇÃO
UFMG
75 ANOS 1950·2025

Sobre a Autora

Ana Cecília Rocha Veiga é Professora Associada do Curso de Museologia da UFMG, pesquisando sobre tecnologia e Web desde 2006. Coordena o Laboratório Virtual LavMUSEU e o Portal Didático Webmuseu. Participou das atividades de *feedback* no desenvolvimento do Manual para Gestão de Coleções Digitais (*Toolkit for Managing Digital Collections*), recurso relacionado do Spectrum, Collections Trust UK, sendo a UFMG a única instituição representada da América Latina. O Spectrum é o padrão do Reino Unido, considerado a principal referência internacional para gestão de coleções e adotado pelos museus ao redor do mundo. Coordenadora Geral do Convênio Internacional de Pesquisa que desenvolveu o projeto Pedras Sabidas: Circuito Acessível de Expositores Interativos no Museu das Minas e do Metal. O projeto Pedras Sabidas foi premiado pelo Programa Ibermuseos, convidado para apresentar uma sessão *como fazer* no MuseWeb em Boston e selecionado pelo Smithsonian Institution para integrar um livro sobre as melhores práticas e pesquisas em interatividade digital inclusiva, sendo o único capítulo selecionado da América Latina. Sua tese de doutorado, publicada no livro Gestão de Projetos de Museus e Exposições, tornou-se bibliografia de concursos públicos e disciplinas diversas de graduação e pós-graduação. Foi Diretora e Vice-Diretora do Museu da Escola de Arquitetura da UFMG (MARQ), sendo ainda sua representante na Rede de Museus da UFMG. Desenvolve projetos e pesquisas em gestão de museus, gestão de acervos, gestão do patrimônio cultural, gestão inclusiva, acessibilidade digital, Tecnologias da Informação e Comunicação (TIC), inteligência artificial, humanidades digitais, neurodiversidade nos museus e nas artes, altas habilidades e superdotação.



Sobre esta pesquisa

Recursos Web para GLAM é um subprojeto da pesquisa *Gestão de Museus e Acervos na Web: TICs*, com integração em extensão e ensino, coordenado pela Professora Ana Cecília Rocha Veiga do Curso de Museologia da Escola de Ciência da Informação da UFMG.

GLAM é um acrônimo em inglês para designar as seguintes unidades de informação e cultura: galerias (*galleries*), bibliotecas (*libraries*), arquivos (*archives*) e museus (*museums*).

Este manual é resultado de nossas pesquisas sobre *Cibersegurança e Privacidade de Dados*, que se iniciaram em 2019. Após longa testagem e divulgação de sua versão Beta, lançamos aqui resultados mais amadurecidos. A maioria das publicações sobre este tema atende a um público altamente especializado, com vocabulários técnicos de difícil compreensão pelos profissionais de GLAM. Procuramos, portanto, sanar esta lacuna com este manual gratuito.

Ainda que não substitua a contratação de consultorias e funcionários especializados no tema, e ainda que seja uma área em constante atualização, este manual pretende, no mínimo, conscientizar gestores de GLAM quanto aos principais desafios que enfrentarão para garantir a segurança cibernética e a privacidade de dados de suas equipes e instituições.

Para obter mais informações sobre este e outros projetos, novas publicações e versões atualizadas deste manual, acesse webmuseu.org

Boas leituras!

Ana Cecília Rocha Veiga – Professora da UFMG

Índice

Sumário

Introdução

Cibersegurança – ou **segurança cibernética** – consiste em ações e recursos para prevenção de ataques cibernéticos e cibercrimes, reduzindo riscos e danos. Atua na proteção dos dispositivos digitais que utilizamos conectados à Internet (celulares, computadores etc.), bem como na adoção de comportamentos que diminuem as nossas vulnerabilidades a estes ataques.

As práticas de cibersegurança objetivam atingir três pilares: **confidencialidade** (proteção dos dados contra divulgação não autorizada), **integridade** (os dados são precisos e não foram alterados de forma não autorizada) e a **disponibilidade** (os dados estão disponíveis para usuários autorizados da forma como prevista).

Tendo em vista estes pilares e suas demandas, profissionais que atuam na área de segurança cibernética estão se tornando indispensáveis. Assim, há toda uma **carreira** possível neste campo para os profissionais de GLAM.

Relacionado ao primeiro pilar, confidencialidade, temos as leis gerais de proteção de dados pessoais – como a LGPD no Brasil e a GDPR na União Europeia. De acordo com estas leis, é responsabilidade das GLAMs, empresas e demais instituições garantirem a segurança cibernética dos dados que coletam de sua comunidade de colaboradores e visitantes. Portanto, cibersegurança e **privacidade de dados** são questões que caminham juntas.

Ano após ano, inúmeros golpes cibernéticos continuam a ser aplicados com sucesso. E o número de fraudes e **crimes** perpetrados via Web está só aumentando. Constatamos neste projeto que não há uma conscientização suficiente acerca do tema.

A situação se torna ainda mais desafiadora quando incluímos uma tecnologia nova e disruptiva nesta equação: a **Inteligência Artificial**.

Por tudo isto, esperamos, com esta publicação, contribuir para tornar nossas GLAMs mais seguras e em conformidade com as leis gerais de proteção de dados vigentes, bem como com os princípios da **ética digital**.

Saiba mais em: webmuseu.org/recursos

Cibersegurança para Usuários da Web

Público-alvo

Qualquer pessoa conectada à Internet se beneficiará da quase totalidade deste checklist, ainda que tenha sido desenvolvido com foco em profissionais de unidades de informação e cultura GLAM (Museus, Bibliotecas, Arquivos e Galerias).

Autenticação de usuários: Login e Senha

Utilizar um **Gerador de Senhas** e um **Gerenciador de Senhas**, como o 1Password, que gera senhas aleatórias e seguras, armazena todos os seus dados de login e senha e os preenche automaticamente nos diversos websites, liberando o usuário de ter que decorar suas senhas. O mercado possui várias excelentes opções disponíveis. Compreendemos ser impossível lidar de forma segura com tantas demandas por logins e senhas sem o uso de um Gerenciador de Senhas. Saiba mais sobre gerenciadores e geradores de senha no FAQ desta seção.

Não utilizar logins repetidos (como e-mails, seu nome etc.) ou padrão (como "admin"), especialmente para a conta de administrador de websites e sistemas. Para usuários de Gerenciadores de Senha, que têm seus dados preenchidos automaticamente pelo software, adote como login um número totalmente aleatório, como se fosse uma senha. Exemplo:

Usuário de login: %ZDSh95SDPR*T4BY@EkC
Senha: tzNbuH4zM8LW#a4Azk#!

Não utilizar sempre o mesmo e-mail em todos os cadastros, sendo aconselhável adotar um e-mail separado para cadastros profissionais e outro para cadastros pessoais, em geral mais arriscados do que os profissionais. Ter sempre, ainda, um terceiro e-mail que possa ser usado para plataformas e serviços menos confiáveis. Alguns serviços de e-mail possuem a opção de utilizar *alias*, que são e-mails apenas para cadastro em newsletters e afins, que não revelam seu e-mail original.

Não utilizar senhas óbvias, como nomes famosos da cultura pop (superman, starwars, batman), cantores (eminem, shakira, justinbieber) jogos (minecraft, pokemon), sequências de letras (querty, as primeiras letras do teclado) ou números (123456). Não utilizar como senha o seu login ou e-mail (isto mesmo, tem pessoas que repetem o login ou o e-mail de cadastro na senha!), variações do seu nome e sobrenome, nome da empresa ou instituição, assunto do website (universidade, museu, facebook etc.), gostos e preferências, datas especiais, nomes de pets etc.

Estudos com banco de dados de senhas vazadas comprovam que muitos usuários utilizam senhas extremamente simples, como estes exemplos acima. E ainda repetem a mesma senha simples em várias contas. **Utilizar senhas fracas ou repetidas é um dos principais motivos pelos quais as pessoas são hackeadas ou sofrem golpes.**

Selecionar **senhas fortes**, preferencialmente geradas randomicamente por *Geradores de Senha*, contendo mais de 12 caracteres, maiúsculas, minúsculas, caracteres especiais e números espalhados ao longo da senha, não agrupados no começo ou no fim.

Exemplo de senha segura: Rk*mFgEy3Bcy

Se não puder criar uma senha complexa, porque necessita decorá-la, escolha uma senha composta por cinco palavras totalmente desconexas (uma *passphrase* - "senha frase"). Uma **senha frase** é melhor do que uma senha insegura. Se puder misturar idiomas diferentes ainda melhor, como este exemplo que inclui "maçã" em alemão (*apfel*) e "cachorro" em inglês (*dog*).

Exemplo: coala-apfel-gol-pegada-dog

Para tornar esta senha ainda mais segura, no lugar dos traços, podemos colocar caracteres em uma lógica fácil de se memorizar. Por exemplo, incluindo os caracteres na sequência do teclado, mas sempre saltando um caractere. O número 3 no final refere-se ao número de cachorros que sua vizinha possui (exemplo fictício), para citarmos alguma referência pessoal de difícil inferência por cibercriminosos:

Exemplo: coala!apfel#gol%pegada&dog3

Selecionar senhas que sejam tecladas com ambas as mãos, dificultando a sua obtenção por observação externa (***shoulder surfing***).

Para fazer uma senha ainda mais segura do que esta, consulte o FAQ dessa sessão.

Nunca repetir uma senha ou variações similares dela. Em caso de hackeamento, o invasor terá acesso a vários dos seus serviços de uma só vez. Não adianta acrescentar no final da senha dicas como "Insta" ou "Face", porque os robôs de hackeamento fazem este tipo de tentativa.

Nunca reaproveitar senhas antigas. Não adianta acrescentar uma ou outra mudança, como um novo caractere ou letra ao final, pois os robôs testam este tipo de reaproveitamento.

Nunca permitir que programas armazenem suas senhas na memória (limpar Histórico do navegador para deletar as eventualmente já salvas). Desmarque a opção de sugerir salvar senhas no navegador da Web, dentre outros softwares que não usem criptografia para armazenar as

senhas. Substitua esta prática pela utilização de um Gerenciador de Senhas, como mencionado acima, que preenche login e senha automaticamente para o usuário de forma segura.

Nunca compartilhar uma conta: cada usuário deve ter as próprias credenciais (login e senha) em todos os serviços. Isto é especialmente importante para atribuição de responsabilidades dentro de um sistema, já que no caso de contas compartilhadas fica impossível saber quem fez qual alteração. É bastante comum, por exemplo, que computadores de instituições GLAM tenham um post it colado, com login e senha do repositório digital, que são utilizados por todos os funcionário e estagiários. Esta prática precisa ser urgentemente banida.

Sempre que possível, **ocultar a senha ao digitar** (selecionar a opção em que a senha aparece na forma de bolinhas ou asteriscos, não visível na tela). Caso digite a senha em algum campo visível, por engano, alterar a senha logo em seguida. Alguns computadores compartilhados ou públicos podem ter softwares que gravam/visualizam a tela ativados.

Se possível, **modificar a senha a cada ano** para as contas mais importantes. Entretanto, dependendo da sua dedicação (ou falta dela) na questão de cibersegurança, é preferível permanecer com senhas seguras por muito tempo do que trocá-las de forma insegura. Veja o FAQ desta seção maiores explicações sobre este tópico.

Alterar a senha imediatamente em caso de vazamento comprovado daquele serviço ou plataforma, substituindo a senha antiga por uma outra senha forte original. Geralmente os Gerenciadores de Senha possuem monitoramento de vazamentos de senhas com seu e-mail ou login. Esteja atento aos seus alertas!

Não clicar nos links de e-mails anunciando vazamentos, pois provavelmente são avisos falsos com links maliciosos. Vá até o site do gerenciador de senhas, plataforma ou serviço hackeado e confirme a informação de vazamento. Na dúvida, aproveite para trocar a senha, mas nunca utilizando o link do e-mail.

Utilizar **autenticação de dois fatores (*Two Factor Authentication* - 2FA ou MFA – *Multi-Factor Authentication*)**, sempre que disponível. A autenticação de dois ou mais fatores, juntamente com senhas seguras, são algumas das principais medidas que garantem a segurança de suas contas. Verifique o FAQ desta seção para mais informações.

Sempre **sair das contas** (efetuar *logout*) ao terminar de utilizar um website, sistema ou serviço on-line. Não permanecer logado sem necessidade. Ao acessar serviços em computadores compartilhados, delete o histórico do navegador ao sair.

Passkeys (Chaves de Acesso): Tecnologia mais segura que senhas

Se puder, substituir as senhas por **passkeys**, que são bem mais seguras do que login e senha. Uma *passkey* é uma tecnologia que utiliza criptografia e dados adicionais (biometria, PIN, desenho padrão, QR Code etc.) para confirmar a identidade de um usuário.

Demanda um celular ou dispositivo eletrônico neste processo, bastando autorizar o uso das **chaves de acesso** nas configurações do equipamento. O Gerenciador de Senhas 1Password também oferece a tecnologia.

É uma técnica não somente mais segura, como também mais rápida para se logar em um website ou plataforma. A *passkey* combina indiretamente a **autenticação de dois fatores (2FA)**, porque certamente o celular ou dispositivo possui camadas de proteção extras de acesso, como senha de desbloqueio ou biometria. (Se não possuir, colocar estas proteções!)

As chaves de acesso funcionam da seguinte maneira, em termos leigos. O local no qual o usuário quer logar possui um cofre (chave pública) que só abre com a chave no celular (chave privada). Ainda que um cibercriminoso chegasse ao cofre, ou seja, invadisse o website ou serviço on-line, não conseguiria fazer nada com este cofre e nem acessar o seu conteúdo salvo dentro dele, porque não tem a chave. E está tudo protegido por criptografia.

A chave está com o usuário, no seu celular ou outros dispositivos autorizados, e ela é "girada" automaticamente na hora de fazer o login, sem precisar de senha alguma. A senha é substituída por esta ferramenta, esta tecnologia de chave de acesso instalada no dispositivo do usuário.

Em geral, os serviços e plataformas que oferecem *passkey* como opção também utilizam em paralelo login e senha. Ou seja, ainda que os cibercriminosos não consigam quebrar uma *passkey*, podem roubar a senha e login para aquela mesma conta. Daí a importância de continuar utilizando autenticação de dois fatores em tudo.

No futuro, talvez tenhamos uma substituição completa do sistema login/senha/2FA por *passkeys*, mas ainda não é uma realidade na maioria dos casos. A *passkey*, neste sentido, é utilizada mais para facilitar o acesso à conta de forma rápida do que para garantir plenamente a cibersegurança, já que os serviços também permitem login com senha convencional.

Segurança dos dispositivos: computadores, laptops e tablets

Não acessar gerenciador de senhas, e-mails, redes sociais da GLAM, painel de controle do WordPress, gerenciador de coleções, dentre outros sistemas relevantes, em dispositivos públicos ou desconhecidos.

Proteger os dispositivos com senha forte de acesso. Vide item específico sobre senhas já apresentado neste manual.

Sempre utilizar **programas originais**, baixados dos websites oficiais. Nunca instalar “piratas”.

Adquirir um potente **antivírus**, malware/spyware e firewall. Utilizamos o McAfee.

Manter todos os **programas e aplicativos atualizados**, em especial sistema operacional, antivírus e navegador.

Deletar todos os softwares e aplicativos que não estejam sendo utilizados, permanecendo somente com o essencial, utilizado com frequência. Caso seja necessário utilizar o software no futuro, ele pode ser simplesmente reinstalado.

Deletar versões antigas de softwares que permitem instalações duplicadas, ficando somente com a mais recente. Geralmente os softwares apagam a versão anterior ao instalar uma nova, o que é a situação ideal.

Trocar os dispositivos eletrônicos por novos sempre que eles não ofereçam condições de comportar versões mais atualizadas do sistema operacional e demais softwares.

Acionar **atualizações e varreduras automáticas** do seu antivírus e demais softwares essenciais.

Realizar inspeções com regularidade nos equipamentos, pelo menos uma vez por ano.

Instalar filtros de privacidade nas telas dos equipamentos (como *3M Screen Privacy Filters*), que dificultam a visualização da tela por quem está ao lado, prevenindo roubo de dados e senhas por observação (***shoulder surfing***). Especialmente importante para quem trabalha em ambientes públicos com seu laptop ou cercado por outras pessoas.

Cobrir entradas de USB e câmeras quando não estiverem sendo utilizadas com frequência, dificultando que invasores tenham fácil acesso presencial ou remoto ao dispositivo.

Esvaziar a lixeira do computador e demais dispositivos sempre que deletar itens, excluindo-os de forma permanente. Principalmente se for algum arquivo infectado ou suspeito.

Acompanhar presencialmente os serviços de manutenção nos equipamentos. No caso de computadores desktop, solicitar manutenção na residência ou instituição, contratando empresa e/ou profissional de confiança.

Proteger o computador com senha de acesso. Sempre que se afastar do computador, ativar novamente o bloqueio de tela, sendo necessário assim redigitar a senha para acessá-lo.

Segurança nos Celulares (*Smartphones*)

Proteger o celular e os principais aplicativos com senhas diferentes (no mínimo 6 dígitos com caracteres variados) e/ou dados biométricos. Não utilizar datas e números óbvios.

Ativar bloqueio automático após 2 minutos sem uso do dispositivo. Não deixar celulares sem supervisão nos ambientes de trabalho e lazer. Muitos golpes podem ser realizados quando o usuário foi ao toalete, por exemplo, e deixou o celular na mesa ou na mochila. Levar o celular sempre consigo.

Encriptar o conteúdo dos celulares, bem como de seus backups na nuvem, de modo com que os dados não possam ser extraídos sem a senha de criptografia, que deve ser uma senha única e forte. Isto é especialmente importante caso o dispositivo seja furtado. iPhone possuem estes recursos de forma facilitada. Lembrar de selecionar alguém de confiança ou salvar a chave de recuperação, caso o usuário perca acesso à conta iCloud.

Apesar de nenhuma empresa no mercado ser plenamente confiável, já que a história nos mostra violações de privacidade de todas elas, iPhones são considerados pelos especialistas mais seguros e privados do que equipamentos com Android. Além disto, a Apple possui recursos avançados de segurança, como o descrito acima e proteção para dispositivo roubado. **Dar preferência a equipamentos Apple, se possível.** Veja no FAQ dessa seção mais informações sobre isto.

Desativar Bluetooth e Wi-fi quando não estiver utilizando, especialmente em ambientes públicos.

Manter o sistema operacional e os aplicativos dos celulares sempre atualizados. Instalar um antivírus, no caso de celulares com Android.

Baixar somente os aplicativos indispensáveis, sempre das lojas oficiais (Apple Store, Google Play etc.) ou fontes extremamente confiáveis. Acompanhar se estes aplicativos não mudaram de dono, passando para mãos de proprietários mal-intencionados que adquirem softwares, plugins e apps de sucesso no mercado para fins ilícitos, alterando-os após a compra.

Conceder permissões aos aplicativos somente quando imprescindível, como acesso às fotos, microfone e localização. Selecionar, ainda, a opção “somente quando o aplicativo estiver em uso”, sempre que disponível.

Desabilitar **geotagging** (marcação geográfica) das fotos e vídeos do celular e/ou remover estes metadados das imagens antes de publicá-las na Internet. Somente publicar localizações em redes sociais quando o usuário não estiver mais no local.

Utilizar aplicativos de mensagens criptografados, como **Signal** (primeira opção), Telegram ou iMessage do iPhone. Ativar mensagens efêmeras, que são as mensagens que desaparecem

depois de um tempo pré-determinado, pois isto não só apaga o histórico, como torna mais difícil o hackeamento e recuperação destas mensagens deletadas posteriormente. Ver FAQ desta seção para mais informações.

Ficar atento aos fóruns e grupos nos quais é incluído nas redes sociais e nos aplicativos de mensagem, bem como ao que compartilha nestes ambientes.

Para assuntos sensíveis, priorizar reuniões presenciais. Reuniões virtuais podem ser gravadas pelos participantes ou mesmo interceptadas por cibercriminosos.

Ambientes físicos também são facilmente grampeáveis, portanto, escolher um local não óbvio para conversar os assuntos mais importantes. Ter em mente que hoje em dia é muito fácil para qualquer um gravar uma reunião.

Se não for possível uma reunião presencial, telefonar ou utilizar chats criptografados privados com tempo de autodestruição, que não salvam as mensagens na nuvem (somente no dispositivo) e as destroem após um período determinado. Evitar vídeos e áudios, dando preferência para texto.

Desativar as notificações de mensagens em telas bloqueadas, que podem ser utilizadas para obter senhas de autenticação de dois fatores, dentre outros dados que aparecem na tela para qualquer um acessar mesmo com o celular bloqueado.

Familiarizar-se com recursos de busca e bloqueio dos celulares, para agir imediatamente em casos de perda ou roubo. Ter consigo anotado em algum local físico o telefone da Central da Apple, caso utilize o iPhone.

Possuir dois equipamentos celulares (e não dois chips no mesmo equipamento), sendo um deles para uso amplo profissional e outro com número pouco divulgado, de acesso restrito. Esta recomendação é especialmente importante para diretores de GLAM. A instituição deveria custear para o diretor um celular profissional. Instalar os aplicativos mais sensíveis e importantes no celular mais restrito.

Se tirar fotografias em ambientes inseguros ou viagens for importante para o usuário, também ter dois celulares: um somente para fotos e vídeos e outro com os dados de banco e aplicativos mais sensíveis e importantes.

Ao adquirir um celular usado ou desfazer-se do equipamento atual, deletar todo o conteúdo e restaurar as configurações de fábrica.

Segurança no Trabalho

Sair das contas ou bloquear o acesso ao computador sempre que deixar a mesa de trabalho, mesmo que por alguns minutos, especialmente em escritórios coletivos.

Não aceitar ajuda de estranhos (suporte, fabricantes, terceirizados ou funcionários desconhecidos), principalmente se tentarem realizar ações (como instalações) que não foram previamente agendadas pela instituição.

Se receber telefonema de alguma empresa ou parceiro fazendo solicitações, informar que irá retornar à ligação. Telefonar, em seguida, para o número que tem costume de se comunicar com aquele prestador de serviços.

Ficar próximo da impressora aguardando a impressão, especialmente equipamentos de uso coletivo ou manuseado por terceiros. Este hábito é crucial quando se tratar de material sigiloso ou importante (por exemplo: planos e cronogramas de transporte de obras de arte de um museu para outro). Configurar a liberação da cópia mediante senha, se disponível.

Picotar envelopes, embalagens de correio e caixas de empresas de entrega antes de descartar no lixo. Além das informações contidas ali (nome completo, endereço etc.), golpistas podem reaproveitar estas embalagens para tentar entrar na instituição disfarçados de entregadores. Raramente profissionais da segurança checam detalhes dos envelopes, como data.

Nunca conversar assuntos sensíveis ou sigilosos no café do museu ou locais próximos da instituição, onde é comum encontrar a equipe almoçando e lanchando. **Engenheiros sociais** (golpistas) procuram estes lugares óbvios para ouvir conversas e coletar informações sigilosas.

Capacitar os profissionais sobre cibersegurança, privacidade de dados e sobre o que pode e o que não pode ser discutido com externos à instituição.

Não descartar documentos e papéis contendo informações importantes (como senhas antigas, planos de exposição etc.) no lixo da instituição, mas fazê-lo em outro local, promovendo antes a sua completa destruição, evitando coletas indevidas (***dumpster diving***). Caso não possua um equipamento fragmentador tipo “confete”, descarte os pedaços em lixos de locais diferentes.

Não descartar DVDs, CDs e computadores antigos sem antes destruir/deletar conteúdo. Destruir completamente a mídia e a descartar nos lixos apropriados para dispensa de equipamentos eletrônicos.

Monitorar os visitantes e funcionários da instituição com a utilização de câmeras de segurança, vigilância humana, alarmes, luzes com sensores de movimento, softwares de monitoramento, uso de senhas para acessar equipamentos e salas especiais etc. Há um conflito evidente entre

privacidade pessoal e segurança no trabalho. E, infelizmente, para aumentarmos a segurança, precisamos reduzir a privacidade. Mas o fato é que ambientes monitorados são menos sujeitos a golpes ou roubos. Informar que o monitoramento existe por meio de placas e manuais de rotina é um dever legal e ajuda a inibir os crimes.

Segurança nas Redes Sociais

Supervisionar detalhes internos divulgados pela equipe de comunicação da instituição nas redes sociais, como montagens de exposições, restauro de obras etc. A instituição se faz vulnerável a ataques cibernéticos com o volume imenso de dados que divulga nas redes ou fornece em serviços e plataformas de IA, muitas delas informações sensíveis.

Ficar atento com “brincadeiras” nas redes sociais, especialmente desafios diversos (citar o nome dos seus animais de estimação, colégio que estudou etc.), pois podem ser utilizados posteriormente para confirmar dados ou tentar adivinhar senhas. Além disto, estes dados vão compor o dossiê que as empresas possuem a respeito do usuário. Não vale a pena conceder o e-mail para *spammers* em troca de uma brincadeira.

Rever configurações de privacidade nas redes sociais, bem como formar listas de contatos separadas para cada tipo de postagem. Em algumas redes sociais é possível classificar quem poderá visualizar cada postagem. Também é possível mudar a privacidade de todas as publicações antigas de uma só vez, alterando-a para “somente amigos”.

Ocultar a lista de amigos e seguidores nas redes sociais, pois cibercriminosos podem tentar chegar até o usuário utilizando informações coletadas a partir de seus contatos.

Conferir todos os contatos que segue nas redes sociais, principalmente nas contas das redes institucionais, pois pode ser um perfil *fake*. E golpistas podem, inclusive, utilizar aquela “amizade” na rede social como credencial para adicionar outros amigos e colegas do mesmo círculo.

Não publicar localização em tempo real, pois isto facilita golpes de todas as espécies. Por exemplo, postar fotografias em cinemas e aviões podem informar aos criminosos que aquela pessoa estará incomunicável nas próximas horas. Isto permite ao golpista entrar em contato com instituições, empresas e pessoas no nome da vítima, sendo que ninguém conseguirá contatá-la rapidamente para conferir se é um golpe em curso.

Segurança na comunicação por E-mails

Utilizar provedores de e-mails que não escaneiam as mensagens, armazenam dados e encaminham propagandas personalizadas. Não recomendamos o uso do Gmail, pois apesar de

excelente em termos de usabilidade, é uma empresa que não respeita a nossa privacidade. Recomendamos configurar em sua empresa de hospedagem de confiança e-mails institucionais utilizando o domínio da GLAM (seunome@nomedomuseu.org). Utilizamos os e-mails e demais serviços da empresa suíça Proton.

Desconfiar caso receba e-mails sobre assuntos que desconhece, respostas para solicitações que não fez, dentre outras correspondências estranhas: a identidade daquela pessoa pode ter sido furtada (***identity theft***) ou seu e-mail pode ter sido falsificado (**e-mail *spoofing***). Reparar se a mensagem contém erros de português inesperados para aquele usuário ou outros detalhes esquisitos.

Ao receber e-mails de pessoas pela primeira vez, buscar na Web o nome da pessoa e o e-mail, para ver se aquele endereço está vinculado a contas de redes sociais estranhas, sites de reclamação etc.

Ao receber novas mensagens que pareçam golpe, mas seja uma mensagem importante e não tenha informações confidenciais, inserir o texto em um chat de IA e pedir para a Inteligência Artificial analisá-lo. A IA pode ser capaz de detectar inconsistências e padrões de golpe. Se o e-mail for em outro idioma que não o seu nativo, pedir para a IA detectar inadequações culturais na escolha do vocabulário. Por fim, submeter a mensagem aos Detectores de IA, para saber se foi mesmo um humano que a digitou.

Fornecer somente dados imprescindíveis à terceiros. Não fornecer e-mail, celular, CPF ou outros dados sensíveis para lojas, websites etc. a menos que tenha plena confiança no serviço e na política de privacidade da empresa. Se não desejar receber mensagens ou e-mails de determinado website ou empresa, não faz sentido fornecer estes dados.

Ativar em gerenciadores de senhas e serviços de e-mails as opções de monitoramento dos dados vazados na ***Dark Web***. Veja o que é a Dark Web no FAQ.

Ativar filtros de spam em e-mails e comentários de websites. Para repositórios e websites em WordPress, recomendamos Akismet.

Não acessar nenhum website via link de e-mails, optando por digitar o endereço no navegador quando precisar acessar um link. Links falsos podem revelar a sua localização exata, instalar vírus ou levar à sites “clonados” que parecem originais, mas não são (**e-mails phishing**). Às vezes o cibercriminoso compra um domínio (endereço URL do site) quase identico ao do site original e, na pressa, o usuário nem percebe que o endereço do site tem uma ou outra letra diferente do oficial.

Configurar o e-mail para pedir autorização antes de executar qualquer ação de e-mails suspeitos: baixar imagens, abrir anexos, liberar Java e JavaScript etc.

No caso de empresas sérias no qual tenha feito cadastro prévio, mas deseje interromper o recebimento de e-mails, solicitar o descadastro via link de descadastramento (em geral, localizado no rodapé de todos os e-mails). Selecionar com atenção os cadastros e newsletters que recebe, por questões de segurança e economia de tempo. Dedicar um e-mail específico para este tipo de correspondência eletrônica, se forem muitas.

Não responder e-mails de spam, pois isto gera uma confirmação para o *spammer* de que o e-mail é válido. Caso não tenha feito o cadastro ou desconheça a empresa que encaminhou o spam, deletar o e-mail e bloquear o endereço.

Evitar responder e-mails "para todos", quando não for imprescindível, bem como ocultar e-mails ao encaminhar mensagens coletivas. Proteger o e-mail dos demais, que devem retribuir a gentileza.

Ocultar e-mails em redes sociais e disponibilizar um e-mail público institucional diferente do e-mail que se utiliza no dia a dia.

Não salvar no Gerenciador de Senhas a senha do seu e-mail principal de cadastro nos diversos serviços, pois em uma emergência (exemplo: esquecimento da senha-mestre do seu software gerenciador, hackeamento do seu gerenciador – o que é bem raro, mas possível), este e-mail principal será necessário para reconfigurar novas senhas nos diversos serviços.

Anotar em um papel suas senhas principais (senha-mestre do gerenciador de senhas, e-mails principais de cadastro etc.) e guardá-las em local superseguro e totalmente secreto em sua residência. Disponibilizar esta informação no seu testamento, se estiver armazenado em um local seguro, e compartilhar este local somente com as pessoas próximas de confiança.

Segurança ao navegar na Web

Utilizar Internet Wi-fi de fonte confiável, não logar em qualquer Wi-fi gratuito ou público disponível na rede. É bem mais seguro acessar a Web pela Internet 5G da operadora de celular do que por um Wi-Fi público.

Trocar o nome padrão e a senha padrão do roteador de Wi-Fi por um nome e senha originais e seguros. Não colocar o nome do usuário ou o nome da instituição, a menos que seja um Wi-Fi público dedicado para visitantes. Por exemplo, o Wi-Fi gratuito disponibilizado para os visitantes de um museu.

Utilizar navegadores que não coletam seus dados e exibem anúncios não solicitados. Utilizamos FireFox e Safari. Para maior anonimato e comunicação sigilosa, utilizar Tor (pode deixar a navegação mais lenta).

Utilizar DuckDuckGo, um mecanismo de busca que não armazena seu histórico de navegação e permite maior customização das permissões. Justamente por não coletar seus dados, dentre outras questões, o mecanismo pode não ser tão "eficiente" quanto o Google, mas para a grande maioria das buscas comuns diárias ele atende perfeitamente ao propósito.

Checar se o website no qual se está logado possui a URL correta (endereço do site, domínio). Sites maliciosos trocam uma ou outra letra da URL e possuem aparência legítima (clones do website original), conforme já vimos neste manual.

Digitar a URL (endereços) de websites importantes, como banco, comércios eletrônicos, serviços de e-mails etc. não acessando estes websites por links ou por resultados de busca em mecanismos como Google. Cuidado com sugestões patrocinadas no Google, pois podem ser sites maliciosos parecidos com os sites originais. Tanto as redes sociais, quanto os mecanismos de busca, não supervisionam corretamente a idoneidade de seus anunciantes. É comum que somente removam *fake news* e golpes somente depois de várias pessoas terem já sido prejudicadas por eles.

Caso estranhe alguma coisa em qualquer website no qual esteja navegando, interromper a navegação imediatamente e telefonar para o setor de TI da empresa/instituição, mesmo que a URL esteja correta. Alguns hackeamentos consistem no sequestro do DNS (domínio, endereço) do website ou redirecionamentos (***pharming***). De posse do endereço legítimo ou de um redirecionamento, o invasor disponibiliza no lugar um website "clone", na tentativa de capturar dados dos usuários (login, senha, conta bancária etc.).

Checar se o website possui conexão encriptada antes de fornecer dados relevantes (como cartão de créditos, dados pessoais etc.), observando, por exemplo, se aparece um cadeadinho ao lado da URL no navegador. Os principais navegadores avisam quando um website não parece seguro ao lado do endereço.

FAQ – Perguntas e Respostas para Usuários da Web

Público-alvo

Qualquer pessoa conectada à Internet se beneficiará da quase totalidade deste FAQ, ainda que tenha sido desenvolvido com foco em profissionais de unidades de informação e cultura GLAM (Museus, Bibliotecas, Arquivos e Galerias).

FAQ – *Frequently Asked Questions*

Qual a diferença entre cibersegurança e segurança da informação?

A *segurança da informação* envolve a segurança de todas as formas de dados em uma instituição GLAM. Já a *cibersegurança* abrange aqueles dados que são armazenados e processados em meio eletrônico.

Por exemplo, a proteção das fichas de catalogação impressas de um museu e guardadas em um arquivo físico é *segurança da informação*. A proteção destas mesmas fichas inseridas no Tainacan ou em outro sistema de gestão de conteúdo digital é *cibersegurança*.

Assim, *cibersegurança* é uma área da *segurança da informação*, mais abrangente.

Para fins deste manual, estamos abordando cibersegurança e segurança da informação de modo conjunto, com enfoque no primeiro. Mas é importante fazer esta distinção.

Qual a diferença entre Hacker e Cracker?

As pessoas em geral e a própria imprensa convencionaram chamar de **hacker** qualquer pessoa que realiza crimes cibernéticos, tais como invasão sem consentimento de sistemas e computadores, obtenção ilícita de informações para ganho pessoal, modificações não autorizadas em softwares e apps etc.

Entretanto, no meio especializado muitas vezes é feita uma diferenciação de nomenclatura. Os “hackers maliciosos” são denominados **crackers** ou **black hat hackers** (hackers do chapéu preto). Enquanto os **gray hat hackers** seriam um meio termo. Por exemplo, um hacker que investiga falhas em um sistema e avisa ao proprietário sobre as falhas encontradas, mas faz isto sem autorização prévia.

Já aquele profissional especialista e autorizado pela instituição, que simula as ações dos *crackers* para identificar falhas de segurança e alertar a comunidade de usuários sobre elas, seria o verdadeiro *hacker*, ou ainda "hacker do bem", "hacker mocinho", **hacker ético** e **white hat hacker** (hacker de chapéu branco).

A denominação "chapéu branco" e "chapéu preto" aparentemente tem sua origem nos filmes de caubói americano, nos quais a cor do chapéu identificava o mocinho e o bandido. Cabe, entretanto, pontuarmos o **racismo estrutural de linguagem** associado à esta definição.

A realidade, contudo, possui um lado cinza, como vimos. Os limites são tênues e, às vezes, explicitamente transgredidos. Muitos *hackers* já foram *crackers* no passado ou mantêm "vida dupla".

O jovem inglês Marcus Hutchins ficou mundialmente famoso por parar o WannaCry, um *ransomware* que bloqueava dados dos usuários e exigia resgate em bitcoins. Posteriormente, foi preso pelo FBI sob várias acusações envolvendo ataques e fraudes bancárias. Em 2019, ele se declarou culpado por ter programado *malware* (contração de *malicious software* – software malicioso).

As Big Techs geralmente possuem times de *hackers* denominados **times vermelhos** (tentam atacar o sistema) e **times azuis** (tentam defendê-los). Esta é uma forma correta de se abordar o problema, empregando hackers éticos que trabalham diuturnamente para o bem do ambiente digital.

É um jogo de "gato e rato", sendo o gato os *crackers* e os ratos os *hackers* éticos. E precisamos ser honestos aqui... no que se refere à cibersegurança, especialmente no campo da Inteligência Artificial, que é uma tecnologia ainda muito imatura, o gato quase sempre sai na frente. E tudo que o rato consegue fazer é minimizar os danos.

Portanto, prevenir ainda é o melhor remédio para diminuir as dores de cabeça em sua instituição e na vida profissional.

Qual a diferença entre crime cibernético e hackeamento ético?

O **crime cibernético** é um hackeamento não ético (crackeamento), como invasão sem consentimento de sistemas e computadores, obtenção ilícita de informações para ganho pessoal, modificações não autorizadas em softwares e apps etc.

Já o **hackeamento ético** é um serviço prestado por especialistas em cibersegurança visando descobrir falhas de segurança em computadores, sistemas e processos. Trata-se de uma investigação autorizada e, em geral, muitíssimo bem remunerada e documentada, seguindo rígidos protocolos.

Por fim, algumas empresas oferecem prêmios vultuosos para qualquer pessoa que quebre sua segurança (e demonstre como o fez), estimulando um ambiente de investigação contínua e escrutínio de seus produtos e serviços. Participar destes concursos é um hackeamento ético. Estes concursos de cibersegurança podem oferecer recompensas milionárias e ajudam a manter nossos apps seguros.

Hackeamento ético também pode envolver a interferência ética não solicitada em GLAMs, para fins pacíficos de protesto (**hacktivismo**) ou produção de conhecimento. Conheça um exemplo de hackeamento ético realizado pela autora deste manual no museu MASP clicando aqui.

Por que o usuário costuma ser o ponto mais fraco da segurança cibernética?

O ponto mais fraco da cibersegurança é, quase sempre, o usuário. Ameaças não maliciosas, como o **erro humano**, estão geralmente presentes nas falhas de segurança cibernética.

Grande parte das pessoas adotam a mesma senha em diferentes contas ou serviços, ampliando o estrago causado quando uma senha ou conta é hackeada.

Para dimensionarmos a gravidade da situação, dados vazados por *crackers* revelam que as senhas mais utilizadas são extremamente fáceis de serem quebradas, sendo algumas adotadas com frequência: 123456, password (senha em inglês) e qwerty, que é a sequência das primeiras letras do teclado.

Crackers munidos de alta tecnologia (softwares e robôs) podem quebrar senhas fáceis como estas em segundos, por meio de **ataques de dicionário** (utiliza como base palavras e senhas comuns), **ataques de força bruta** (por tentativa e erro de todas as combinações possíveis) ou **ataques arco-íris** (utilizam tabelas pré-calculadas para adivinhar a senha, aumentando a velocidade da quebra).

Senhas e dados confidenciais podem, ainda, ser obtidos com baixa tecnologia, por exemplo, observando o usuário digitar (***shoulder surfing***) ou se passando por empresas em telefonemas. São os chamados golpes de engenharia social.

O que é engenharia social e por que ela é tão perigosa?

Engenharia social é o hackeamento com baixa tecnologia. Falando em termos leigos, são táticas para ludibriar as pessoas, fazendo-as revelar informações sigilosas ou agirem de modo contrário ao que fariam se percebessem que estão sendo enganadas.

Trata-se de **golpes** extremamente comuns que causam prejuízos incalculáveis às pessoas, empresas e instituições, todos os anos.

Estes golpistas lançam mão de técnicas da psicologia para persuasão, tais como **prova social** (repetir comportamentos dos demais funcionários da instituição para se inserir), **autoridade** (cargos e títulos acadêmicos falsos, roupas caras, citar nomes de pessoas importantes, uniformes institucionais ou policiais etc.), e **simpatia**.

As pessoas compartilham toda sorte de informações pessoais na Web e nas redes sociais. Além disto, currículos como LinkedIn, Lattes ou plataformas de genealogia familiar fornecem aos golpistas uma quantidade absurda de informações que podem ser utilizadas para enganar o usuário, seus colegas, amigos e parentes.

Alguns trabalhos envolvem muita exposição pública na Web. Acadêmicos, escritores, curadores, professores universitários, diretores de instituição GLAM, dentre outras categorias, com frequência têm a sua agenda pública.

Por exemplo, se um museu anuncia em suas redes sociais um congresso com convidados de fora, de outras cidades, sabemos automaticamente que estes palestrantes não estão em sua residência ou instituição GLAM. Só esta informação já é suficiente para facilitar desde invasões físicas ao local, quanto golpes. O golpista pode descobrir a hora do voo do palestrante e, enquanto ele está incomunicável no avião, realizar um "sequestro virtual" (fingir para seus parentes ou colegas que a pessoa está sequestrada) ou se passar por ela em telefonemas e até presencialmente.

Por estes motivos, os profissionais de GLAM que realizam procedimentos de rotina na Web, tais como atualizar o website da instituição ou alimentar o sistema de gestão das coleções, precisam estar preparados para assumir protocolos responsáveis de segurança cibernética, como os sugeridos neste projeto. E isto inclui se preparar para não cair em golpes de engenharia social.

Não tenho condições de seguir tantas recomendações de cibersegurança. Quais destes procedimentos são mais importantes e totalmente imprescindíveis?

Um dos pontos inegociáveis é o uso de **senhas fortes**. Portanto, utilize senhas longas e únicas para cada serviço, contendo vários tipos de caracteres (letras, números, caracteres especiais), bem como **autenticação de dois fatores (2FA)**.

Para quem possui muitas contas (redes sociais, serviços, comércios etc.), ou seja, provavelmente todos os leitores deste manual, a única solução eficiente é adotar um **Gerenciador de Senhas**. Com um Gerenciador é possível salvar senhas ainda maiores, com 25 a 30 caracteres aleatórios, de forma segura e criptografada.

Cada usuário deve, ainda, possuir seu **login e senha individuais** na instituição e ter as suas atividades rastreadas. Diversos softwares e sistemas, como o Moodle, WordPress e o Tainacan, permitem recursos de registros de login e atividades dentro do software.

Jamais deixe um post it com login e senha no computador institucional, permitido que todo mundo compartilhe as mesmas credenciais! Isto é extremamente comum e altamente perigoso.

Por fim, garanta que os dispositivos (computadores, celulares etc.) possuam somente **softwares e apps originais, sempre atualizados**. A desatualização é uma das principais causas de fragilidade da segurança na Web.

No caso de computadores, um **software antivírus** profissional também é indispensável.

O que é um Gerenciador de Senhas?

O **Gerenciador de Senhas** é um software que armazena, criptografa e preenche para o usuário login e senha automaticamente nos websites, contribuindo para que todas as senhas sejam fortes e únicas, já que não será mais necessário memorizar nenhuma senha, com exceção da "senha mestre" (a que concede acesso ao cofre de senhas). Nos equipamentos com biometria, nem é necessário ficar digitando a senha-mestre.

Uma vez logado, o Gerenciador preenche automaticamente os dados de acesso em qualquer website, sem a necessidade de digitar nada, em apenas um clique. Basta selecionar o website desejado e o login é realizado instantaneamente. Para isto o Gerenciador de Senhas utiliza aplicativos (celulares e desktops) e extensões (plugins instalados no seu navegador).

Além de senhas, o Gerenciador também preenche formulários de cartão de crédito e endereços, cria senhas seguras em novos cadastros, podendo alterar senhas antigas por outras automaticamente. Alguns gerenciadores também permitem incluir anotações e arquivos nos seus cofres. Oferecem, por fim, planos coletivos para famílias ou empresas, nos quais familiares ou funcionários podem ter seus cofres particulares e outros compartilhados com os demais.

Gerenciadores de Senha realizam checagens nas senhas dos cofres, identificando falhas de segurança e sugerindo correções nas senhas frágeis, mudanças em senhas vazadas etc.

Utilizamos o **1Password**. Mas existem várias outras opções seguras no mercado.

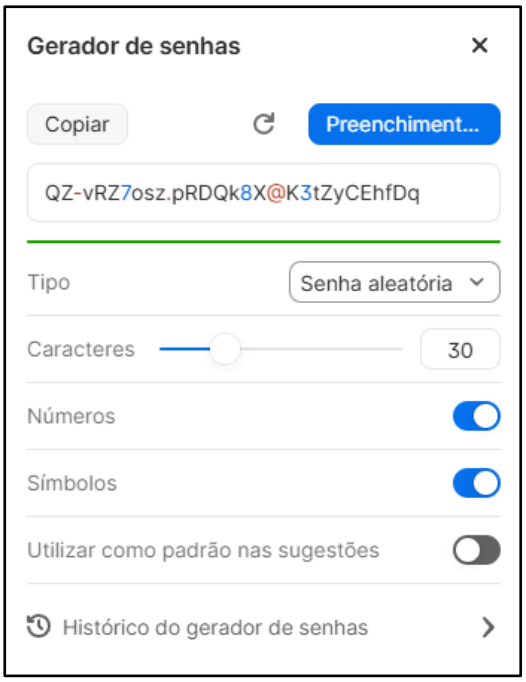
A única maneira de se ter senhas realmente únicas e seguras para tantas contas que possuímos hoje em dia é por meio de um Gerenciador de Senhas. É uma das medidas mais importantes que um usuário ou uma GLAM pode tomar em termos de cibersegurança.

O que é um Gerador de Senhas?

Um Gerador de Senhas é um software que gera senhas totalmente aleatórias, de acordo com o número de caracteres solicitado. Geradores são capazes de produzir senhas complexas e indecifráveis, tais como: uf9edqYfFAmxu9zqn_LT!X6VNiWp-f

Alguns ajustes podem ser selecionados, como **senhas fáceis de ler** (sem caracteres ambíguos do tipo número “O” e letra “o”) e **fáceis de pronunciar** (evita números e caracteres especiais).

Contudo, o melhor para a segurança é utilizar todos os tipos de caracteres: maiúsculas, minúsculas, dígitos e símbolos. Para não se preocupar em memorizar senhas, utilize um Gerenciador de Senhas.



Fonte: Gerador de Senhas do 1Password

Como criar uma senha segura e memorizável para ser a senha-mestre do meu Gerenciador de Senhas?

Neste manual já explicamos como criar senhas seguras. Como se trata da senha mestre, ou seja, a senha que protege todas as suas senhas, vamos adicionar algumas camadas a mais de complexidade. Mas a vantagem é que esta será a única senha que você precisará decorar.

Dentre todos os cuidados, dois fatores jamais podem ser negligenciados numa **senha-mestre: o seu tamanho e sua exclusividade**.

Uma senha forte e segura é longa, com 20 ou mais caracteres. Também precisa ser única, jamais reutilizada em outra conta, mesmo com variações em torno da senha principal.

Um caminho eficiente para se criar uma senha-mestre memorizável é escolher uma frase. Mesmo o mais potente computador, executando um excelente software robô invasor, demoraria uma eternidade para quebrar uma senha composta por uma frase longa (***passphrase***).

Para ser segura, precisa preferencialmente ser uma frase de pelo menos cinco ou seis palavras randômicas (ex: coala, modernismo, chuva, tinta, literatura, *apfel*). A frase pode ser, ainda, entremeada por números, caracteres especiais, maiúsculas e minúsculas. Se forem adicionadas palavras em outros idiomas ainda melhor, como neste exemplo, *apfel* é maçã em alemão.

Substituir caracteres por letras parecidas é uma tática fraca, pois os robôs fazem essas simulações em seus ataques. O ideal é incluir alguns caracteres aleatórios, mas se combinada com uma *passphrase*, esses caracteres fáceis de memorizar podem ajudar a dificultar a senha:

%coa!amoderni$moChuvatint@literatura*apfeL

Frases que façam sentido gramatical, como "*Monet pintou quadros impressionistas*", não são seguras. As palavras precisam ser desconexas uma das outras.

Se a frase for popular, como uma música ou um poema, pode-se optar pelas três primeiras letras de cada palavra de um verso. Assim, será mais difícil esquecê-la e ainda mais difícil quebrá-la do que palavras que existam em um dicionário, letras de músicas etc.

O ideal seria selecionar uma frase que faça sentido somente para o próprio usuário. O usuário pode estruturar uma história que tenha significado pessoal, facilitando a memorização, mas que ninguém consiga decifrar.

Por exemplo: *O Marcos não devolveu dois livros! Amigo… quero de volta, por favor*. Contando essa história com as três primeiras letras de cada palavra, inserindo randomicamente os caracteres especiais e números, a senha forte ficaria assim:

oMarnaodev2liv!Ami…quedevol,porfav.

A senha acima demoraria 20 septendecilhões de anos para ser quebrada. Após criar a senha, os Gerenciadores de Senha a testarão para você, apontando possíveis fragilidades.

Anote esta senha em um local superseguro e não digital, com papel e lápis, sem dar maiores contextos. E esconda em um local de difícil acesso em sua residência. Coloque a informação no seu testamento, se este documento estiver armazenado em local seguro, e informe o local do esconderijo somente para as pessoas mais próximas e confiáveis.

Troque sua senha mestre a cada ano por outra igualmente segura, que nunca tenha sido utilizada antes. Se não se sentir seguro para criar e decorar uma nova senha, é preferível manter a senha antiga e adicionar algum caractere no meio da senha (jamais no final) do que simplesmente não mudar a senha mestre nunca.

Por fim, não a salve automaticamente em nenhum navegador ou celular pois, além de ser um procedimento inseguro, ter que digitar sua senha diariamente auxilia no processo de memorização.

Uma vez esquecida sua senha-mestre, você simplesmente perdeu todas as senhas de seu cofre. Nem a empresa do Gerenciador de Senhas é capaz de obter a senha para você, pois é tudo criptografado. E é justamente isto que garante a segurança dos seus dados!

Preciso mesmo mudar a minha senha após alguns meses de uso?

Uma senha longa e forte é capaz de resistir a ataques randômicos de robôs. Entretanto, em um ataque direcionado, no qual um invasor foca em um único alvo, quebrar a senha é uma questão de tempo e recursos, em geral por meio de **ataques de força bruta** (tentativa e erro até o computador conseguir adivinhar a senha).

Se alterarmos a senha, por exemplo a cada seis meses ou a cada ano, o invasor precisaria começar o ataque do zero novamente a cada troca. Se mantivermos senhas fortes e as trocarmos com frequência, tornamos a invasão por este meio quase impossível.

Na prática, contudo, as recomendações de se alterar as senhas com frequência têm sido revistas, pois os usuários criam o hábito de anotar as senhas em locais fáceis de achar, bem como podem substituir a senha anterior por outra de fácil memorização ou alguma senha antiga, resultando em um cenário geral pior do que manter a senha antiga forte. Afinal de contas, ataques de longa duração direcionados a uma conta específica são mais raros, a menos que sua instituição seja muito importante ou você tenha um cargo público muito visado por cibercriminosos.

Alguns gerenciadores de senha possuem serviços de mudança automática de senha. Agências governamentais que lidam com dados altamente sigilosos podem solicitar/automatizar a mudança de senha automaticamente a cada acesso. Creio que não seria o caso das GLAMs.

Portanto, como regra geral, podemos dizer que mudar a senha de tempos em tempos, por exemplo, após alguns meses ou anos, pode ser uma boa. Porém, mais importante do que mudar a senha com frequência é agir de modo cauteloso e manter senhas difíceis de serem adivinhadas ou quebradas.

Caso tenha certeza de que alguém tentou logar sua conta com a sua senha, ou caso seja avisado pela imprensa ou pelo próprio serviço de que senhas foram vazadas, neste caso, é preciso mudar a senha imediatamente. Se for avisado de algum problema na sua conta ou vazamento por e-mail, não clique no link, pois provavelmente é uma mensagem falsa. Vá até o seu monitor de vazamento (ex: gerenciador de senhas), ou site da empresa supostamente hackeada, e confira se há mesmo um anúncio de vazamento.

O que é Autenticação de Dois Fatores (2FA) ou de Múltiplos Fatores?

A autenticação de dois fatores (***Two-factor Authentication***) exige uma confirmação além da senha, garantindo deste modo que o usuário seja realmente o dono da conta. A autenticação de Múltiplos Fatores (***MFA – Multi-factor Authentication***) conta com dois ou mais processos de autenticação. Por exemplo, senha, aplicativo de 2FA e biometria.

Esta confirmação pode ser algo que **você sabe** (uma informação extra), algo que **você tem** (uma senha enviada para o seu celular por SMS ou gerada por aplicativo 2FA) ou algo que **você é** (dados biométricos, como sua face ou digital).

Confirmações por SMS não são as mais recomendáveis, pois podem ser facilmente crackeáveis de diversos modos. É preferível utilizar aplicativos geradores de senhas temporárias para autenticação 2FA.

Estes aplicativos geram novas senhas a cada 30 segundos e são facilmente vinculáveis às contas por meio de QR Code. Um exemplo de app gratuito de 2FA é o **Microsoft Authenticator**.

Por que dispositivos Apple em geral são considerados mais seguros?

A primeira razão pela qual equipamentos Apple costumam ser considerados mais seguros é porque são menos utilizados do que os demais. Assim, muitos *crackers* preferem dedicar o seu tempo a produzir vírus e robôs que ataquem PCs e Androids, ampliando suas chances de uma invasão bem-sucedida. O Android é o sistema operacional mais utilizado em todo o mundo. A maioria dos celulares o utilizam.

O segundo motivo consiste no fato de que a obtenção dos dados para revenda não faz parte, pelo menos de forma central e explícita, do negócio da Apple, ao contrário do que se observa na empresa Google (gestora do sistema operacional Android), uma empresa que abertamente capitaliza nossos dados e que não prioriza a privacidade como modelo de negócio. A Google faz parte do que chamamos de **Capitalismo de Vigilância** e **Economia da Atenção**.

Contudo, às vezes os próprios sistemas de privacidade da Apple podem conter vulnerabilidades que expõem dados dos seus usuários. Não existe empresa de tecnologia perfeita e nem totalmente confiável neste quesito, infelizmente.

O terceiro é o fato da cibersegurança ser um dos lemas de *marketing* da Apple, que cobra mais caro por seus produtos, também, por oferecer um ambiente mais seguro para seus clientes.

Por exemplo, inserir aplicativos na Apple Store é um processo caro e demorado, além de mais rigoroso do que na Google Play. As configurações padrão dos produtos e aplicativos para

equipamentos Apple também são mais restritivas e customizáveis por leigos do que as para Android/PCs.

É simples criptografar laptops e demais dispositivos Apple, exigindo poucos cliques e pouco conhecimento técnico para isto.

O iPhone possui vários recursos extras contra roubo. Se esta proteção extra estiver ativada, será necessário esperar uma hora e conferir novamente a biometria antes de prosseguir com alterações mais sérias, como mudança de ID. Em caso de roubo, é simples o procedimento para bloquear o celular. Por fim, mesmo dispositivos mais antigos ainda são capazes de rodar as versões mais atualizadas do sistema operacional e aplicativos. Isto nem sempre se verifica nos celulares Android, que podem perder rapidamente a capacidade de atualizar o sistema operacional à medida que envelhecem. Por diversos motivos, sendo estes somente alguns, equipamentos Apple costumam ser mais seguros do que os demais.

Infelizmente a marca tornou-se objeto de desejo e status, encarecendo ainda mais seus produtos e explorando este lado deplorável da tecnologia, que é a **obsolescência programada** e a **obsolescência percebida**. Sobre este assunto, recomendamos fortemente o documentário A História das Coisas (legendas em português).

Foge ao escopo deste FAQ nos delongarmos no controverso debate “PCs x Macs” e “Android x iOS”. Não obstante a Apple ser uma empresa extremamente proprietária, de baixíssima interoperabilidade, valores altamente questionáveis, passível de inúmeras críticas, se a segurança for um fator importante e puder arcar com os custos, privilegie equipamentos Apple.

Por que o Signal foi considerado mais seguro do que o Telegram e do que o WhatsApp?

O que estes três aplicativos têm em comum – Signal, Telegram e WhatsApp – é que, se bem usados, são extremamente seguros, pois criptografam as mensagens de ponta a ponta, garantindo que não sejam interceptadas e decifradas no caminho e nem no servidor.

Por isto, quando o Telegram ou o WhatsApp afirmam que não podem fornecer suas mensagens para a justiça, em caso de solicitação, é porque eles efetivamente não podem (no caso do Telegram, os chamados “chats privados”, como veremos a seguir). No Telegram a criptografia não é o padrão, mas uma opção do usuário. Caso opte por chats sem criptografia, as mensagens poderão ser lidas em mais de um dispositivo e ficarão armazenadas na nuvem da empresa por um tempo determinado. Isto não torna o Telegram mais inseguro, apenas significa que o usuário precisará decidir o grau de privacidade que deseja para cada comunicação específica.

O Telegram utiliza, porém, alguns recursos controversos de criptografia. Apesar das críticas, até

hoje ninguém obteve nenhum dos prêmios oferecidos nos seus concursos de segurança, que chegaram a oferecer $300 mil dólares para quem quebrasse o aplicativo e mostrasse como o fez. Contudo, os valores questionados associados à empresa e seus criadores, bem como o seu uso por criminosos, tem feito as pessoas abrirem mão deste app.

Dos três, somente o WhatsApp não possui nada em código aberto, o que impede que conheçamos plenamente o seu funcionamento, bem como que auditores externos identifiquem falhas de segurança, que poderiam ser corrigidas mais rapidamente. Além disto, o WhatsApp pertence ao Facebook e monetiza nossos dados, o que significa que suas informações de uso do aplicativo estão alimentando o lucro e o "dossiê" que a empresa Meta dispõe sobre você. Apesar de não poder ler o conteúdo das mensagens criptografadas, a empresa coleta metadados do usuário e os integra aos que já foram obtidos via Facebook e Instagram.

No caso do **Signal**, o aplicativo não é comercial e é o único cujo servidor também possui código aberto, ampliando ainda mais a transparência. Não localizamos casos de hackeamento deste aplicativo. O seu protocolo de criptografia ponta a ponta foi adotado pelo Facebook, WhatsApp, Skype e Google, o que só reforça o seu prestígio.

O Signal é geralmente considerado o **mais seguro de todos** por especialistas em cibersegurança, por isto tem sido adotado por ativistas e políticos no mundo todo. Especialmente quando as mensagens efêmeras, que desaparecem depois de um tempo pré-determinado, estão ativadas. Desde modo, é ainda mais difícil para um hacker com acesso a softwares forenses conseguir recuperá-las do seu aparelho. O Signal não armazena suas mensagens na nuvem.

Em resumo, todos os três são seguros, mas após analisar as avaliações dos especialistas e testar os mensageiros, recomendamos o **Signal**. Para quem possui equipamentos Apple, o **iMessage** também é excelente aplicativo e possui criptografia de ponta a ponta.

Nada impede, entretanto, que hackers sofisticados façam hackeamento do celular como um todo, acessando tudo que acontece nele remotamente por meio de um software Pegasus. Entretanto, este tipo de espionagem mais sofisticada é bem mais rara de acontecer com pessoas comuns, mas sim com autoridades importantes ou funcionários com altos cargos em grandes empresas.

Por que devo ficar atento aos grupos públicos dos quais faço parte?

Primeiramente, muitos usuários não têm noção do quão público são os grupos dos quais participam. Muitos fóruns e grupos de Facebook requerem solicitação de participação, mas seus dados podem ser visualizados por qualquer um.

Além disto, usuários e empresas podem extrair os comentários e dados do grupo, segmentando seus participantes de acordo com suas opiniões, medos, interesses etc. A partir disto, novos

grupos são criados objetivando bombardear estas pessoas com informações para as quais estejam susceptíveis, ampliando os efeitos de manipulação (compra de produtos, guerras culturais, políticas etc.).

Por fim, um grupo que é privado hoje, pode ser público amanhã. Uma pessoa que não participava do grupo pode passar a fazer e acessar, em muitos casos, conteúdos antigos.

Grupos na Web não são seguros e são alvos frequentes de investidas dos *crackers* na obtenção de informações sobre usuários, empresas e instituições. Tenha muita responsabilidade ao postar informações pessoais ou da sua GLAM em grupos públicos nas redes sociais e na Web.

Por que devo ter dois equipamentos celulares?

Pessoas públicas, cujos números precisem ser amplamente difundidos, devem possuir dois equipamentos distintos, sendo um restrito para pessoas de confiança. A obtenção do número do celular facilita hackeamentos diversos, bem como esquemas de **engenharia social** (golpes).

Uma prevenção contra isto seria concentrar no equipamento de uso restrito os recursos mais relevantes no que tange à segurança, como aplicativos de rotina, bancários, gerenciamento de coleções on-line e projetos, 2FA (autenticação de dois fatores), dentre outros.

No caso de pessoas em altos cargos, como diretores de GLAM, a instituição deveria custear um equipamento para uso profissional, mantendo o diretor um celular pessoal reservado aos contatos mais próximos.

Por que publicar os bastidores das GLAMs nas redes sociais fragiliza a segurança?

O marketing digital é, hoje, parte importante da estratégia de comunicação das principais instituições do mundo. Entretanto, precisamos estar cientes de que esta superexposição revela dados essenciais que podem ser utilizados por golpistas (engenheiros sociais), como modelos dos uniformes e crachás utilizados pelos funcionários, empresas terceirizadas contratadas, cronogramas, procedimentos, nomes de funcionários e pessoas envolvidas etc.

Portanto, é preciso pesar prós e contras e analisar se a instituição tem condições de arcar com as demandas de segurança geradas por esta divulgação. Se a sua GLAM não possui sistemas eficientes de segurança física e cibernética, não exponha seus bastidores na Web, nem fotografias de acervos que possuam alto valor monetário ou social.

O que é *Deep Web e Dark Web*?

A **Rede Profunda** (*Deep Web*) é o conteúdo on-line não-indexado pelos mecanismos de busca e que não faz parte da *Surface Web*. Representa, na verdade, a maior parte absoluta da Web. Trata-se de tudo aquilo que está protegido por uma senha, como seu e-mail, ou por um *paywall*, como jornais e cursos on-line pagos.

Já a **Rede Sombria** (*Dark Web*) é uma parte da *Deep Web* focada em total privacidade. Foi criada nos anos 90 pelo Departamento de Defesa dos EUA, para que seus espiões pudessem se comunicar em sigilo. Em 2004, ela se tornou pública, abrindo portas para que criminosos se aproveitassem deste anonimato.

Para acessar a *Dark Web* é preciso utilizar softwares especiais, como o navegador Tor. E, em alguns casos, receber um convite/autorização para acesso daquele conteúdo específico. Por estas razões, muitas vezes a *Dark Web* é utilizada para fins ilícitos, como venda de drogas, vazamento de dados hackeados etc.

Entretanto, nem todo uso da *Dark Web* é ilegal ou ilegítimo. Jornalistas e ativistas sociais que residem em países ditatoriais podem optar pela *Dark Web* por causa da necessidade de **anonimato**.

Para garantir este anonimato, as redes da *Dark Web* lançam mão do roteamento indireto e criptografia em múltiplas camadas, protegendo assim a identidade de seus usuários.

O que é criptografia?

A criptografia é um processo que torna cifrado um texto simples, por meio de algoritmos e modelos matemáticos criptográficos. Assim, somente as pessoas autorizadas serão capazes de ver aquele conteúdo.

Os principais objetivos da criptografia são a **confidencialidade**, a **integridade** da informação transmitida, a **autenticidade** e o **não repúdio**. Estes dois últimos garantem que os dados não sejam alterados e, também, que não tenham a sua origem negada por quem os criou ou enviou.

Todos nós utilizamos criptografia o tempo todo sem percebermos. Por exemplo, ao realizarmos uma transferência bancária no celular ou acessarmos um website protegido, daqueles que têm um “cadeadinho” ao lado da URL no seu navegador.

Ainda que seja difícil de entender para um leigo, o resultado da criptografia é simples: sempre que seus dados forem criptografados, eles estarão infinitamente mais **seguros**.

Como saber se a conexão com um website é encriptada e segura?

A maioria dos websites de maior porte atualmente fornecem conexão encriptada, sendo alguns indícios de que a conexão é segura:

- O website se inicia com https (com um S incluído no final).
- O website está marcado pelo navegador e/ou pelo mecanismo de busca como conexão segura (verde).
- O navegador exibe um cadeado fechado ao lado da URL do website, em vez de “Não seguro” ou avisos similares.

Como saber se meu computador ou celular foi hackeado?

Qualquer alteração estranha em um dispositivo eletrônico deve ser observada e acompanhada com atenção. Eis algumas delas:

- O equipamento está mais lento do que o normal.
- Aparecem novas configurações, apps ou softwares sem o seu consentimento.
- A bateria descarrega rápido demais.
- O dispositivo fica mais quente do que o normal com frequência.
- Somem arquivos ou eles são movidos para a lixeira sem o seu consentimento.
- Softwares começam a funcionar de forma intermitente ou dar “problema”.

Cibersegurança para Gestores de GLAM

Público-alvo

Qualquer gestor de instituição, universidade ou empresa que possua TI se beneficiará da quase totalidade deste checklist, ainda que tenha sido elaborado com foco nas GLAMs (museus, bibliotecas, arquivos e galerias).

Prevenção contra Ameaças Internas

Checar o **passado dos novos funcionários** e/ou usuários de sistemas da instituição, incluindo ficha criminal, conhecimentos prévios de informática, currículo, redes sociais e referências. Manter estes dados mesmo após o desligamento do colaborador.

Priorizar a contratação de colaboradores que tenham **inteligência emocional e habilidades leves (*soft skills*)**. O conhecimento objetivo do trabalho é mais fácil de ser adquirido. Qualidades como ética profissional e disciplinas são muito mais difíceis de serem ensinadas.

Caso a GLAM não possua um setor de Recursos Humanos estruturado, contratar empresas de **consultoria em RH** para a seleção dos candidatos a vagas de emprego na instituição. Testes psicológicos e avaliações psiquiátricas devem estar incluídas neste processo, além da já mencionada checagem de currículo e investigação de antecedentes criminais.

Não subestimar funcionários com comportamentos profissionais antiéticos, vingativos e/ou sem comprometimento para com a equipe e função social da instituição (inteligência emocional, habilidades leves – *soft skills*). Grande parte dos cibercrimes contam com a participação de funcionários ou ex-colaboradores.

Desabilitar as contas de e-mail e de acesso de ex-funcionários e ex-voluntários aos sistemas da GLAM assim que forem desligados da instituição. Manter as informações de credenciais do funcionário/voluntário salvas em um banco de dados, mesmo após desligamento.

Manter um **cadastro completo** de todos os funcionários e voluntários da instituição, bem como de ex-funcionários e ex-voluntários, anotando quando e o que fizeram enquanto estavam na GLAM.

Elaborar uma criteriosa **classificação de acesso** aos dados e funções nos softwares, concedendo a cada usuário somente os perfis indispensáveis para a realização de suas atividades de rotina.

Instalar softwares/plugins de monitoramento de atividades em websites, coleções on-line, dentre outros sistemas relevantes na rede da instituição. Assim, tudo que cada usuário fizer ficará devidamente registrado (logs). A maioria dos sistemas de gestão para GLAM já possui esta função no *core* (instalação padrão).

Instalar softwares/plugins que possuam controle de versões (**version control**), permitindo, além da identificação das alterações realizadas por cada usuário, também o retorno para versões anteriores, se necessário.

Manter data e horário corretas nos computadores e demais dispositivos, para adequado registro dos *logs* (atividades realizadas).

Gerar periodicamente relatórios de atividades para análises e **auditorias**.

Cultivar uma cultura de **gerenciamento de risco** (*culture of risk management*), promovendo sempre discussões sobre o tema e capacitação da equipe.

Segurança na Comunicação

Para questões internas profissionais da instituição, utilizar aplicativos seguros de gestão virtual, livres de coletas e repasses de dados, bem como de algoritmos, evitando serviços "gratuitos", como Google (Gmail, Google Calendar, Google Drive etc.). A melhor opção, quando possível, é não utilizar programas comerciais e estruturar sua própria plataforma de gestão com softwares código aberto, como **intranet em WordPress**. Deste modo, os metadados de uso do software não serão repassados a nenhuma empresa.

Dentre as opções comerciais, utilizamos o **Basecamp** (gestão de equipes) e o **Todoist** (gestão da produtividade pessoal do gestor).

Não utilizar redes sociais comerciais para organização da comunicação interna do museu, como grupos de Facebook, Instagram etc. Com plugins como BuddyPress e bbPress é possível desenvolver sua própria rede social em WordPress, privada e livre de algoritmos e propagandas.

E-mails da instituição devem ser utilizados apenas para questões profissionais. Instruir funcionários a manterem uma conta pessoal em separado para assuntos privados, evitando abri-la nos computadores da instituição. Empresas de e-mails como a Proton possuem comunicação criptografada, privada e segura, ao contrário do Gmail, que não respeita a nossa privacidade.

Instruir os funcionários a não abrirem e-mails não solicitados, especialmente de estranhos, não clicando em links ou abrindo anexos não esperados.

Documentos digitalizados e disponibilizados no website da instituição não devem possuir assinaturas, carimbos ou timbres internos (prevenção contra falsificações). Dê preferência para assinaturas digitais, como a disponibilizada gratuitamente pela plataforma SouGov.

Segurança física e prevenção de ataques externos

Possuir recepcionistas, registro de entrada e saída de pessoal e sistemas de segurança (alarmes, câmeras etc.) na instituição.

Sempre acompanhar visitantes nas áreas técnicas e administrativas da instituição, que devem ser identificados e registrados na recepção.

Sempre acompanhar equipes de limpeza em áreas técnicas e administrativas da instituição. Serviços de manutenção não devem ser realizados sem a presença de uma pessoa responsável da instituição 100% do tempo.

Limitar e vigiar o acesso às salas administrativas e escritórios da instituição, que devem ser acessíveis somente aos funcionários autorizados (trancar com chaves multiponto, cartões, senhas etc.).

Adotar um uniforme para a equipe da instituição ajuda a identificar quando uma pessoa de fora está adentrando áreas não autorizadas. Além disto, dificulta golpes, pois os criminosos precisarão roubar ou produzir uniformes iguais/similares.

Remover placas indicativas como “Sala de informática”, “Reserva Técnica”, “Laboratório de Conservação”, etc., que indicam para estranhos onde e como tudo funciona na instituição. Quem trabalha na GLAM sabe onde fica cada setor e não precisa disto para se localizar no dia a dia. Outra opção é colocar nomes genéricos, por exemplo, em um museu literário, sala “Guimarães Rosa”, “Cecília Meireles”. Assim fica fácil indicar para visitantes qual sala ele deve procurar.

Garantir a segurança da sala de informática com portas e fechaduras fortes, janelas com grades, câmeras e alarmes. Somente pessoal autorizado deve ter acesso.

Manter equipamentos e backups em cofres ou, no mínimo, armários trancados. Dados extremamente sigilosos devem ser processados e armazenados em computadores desconectados da Internet.

Manter equipamentos afixados nas mesas com travas, especialmente laptops com conteúdos importantes ou sensíveis, impedindo roubos e remoções não autorizadas.

Não “emprestar” ou facultar o uso de equipamentos para pessoas de fora da instituição ou mesmo funcionários que não tenham treinamento nos protocolos de segurança da instituição.

Criptografar discos rígidos de computadores, laptops, HDs externos e pen drives. Utilize **Vera Crypt** (software gratuito que atende a vários sistemas operacionais), **BitLock** (Windows/Pacote Office).

Proteger a rede e os pontos wireless LANs (redes sem fio locais, também chamadas de Wi-Fi). Garanta que o sinal não seja forte o suficiente a ponto de ser captado pelo público externo ao edifício, a menos que essa seja a intenção (democratizar acesso à Internet via instituição). Neste caso, reforce os cuidados com a segurança cibernética.

Possuir **geradores e *nobreaks***, que são equipamentos que mantém as luzes de emergência e os computadores funcionando por um tempo, até que a energia volte. Ativar modo ***fail closed*** (o acesso aos computadores será restrito aos Administradores até que o fornecimento de energia se normalize).

Quando possível, designar um equipamento exclusivo para realização de atividades críticas, como atualizar sistemas de gestão de coleções on-line, softwares de bibliotecas e arquivos, websites etc. Bloquear neste computador o acesso à websites desnecessários à estas atividades essenciais (ex: gmail, jogos e redes sociais).

Realizar o mapeamento dos riscos (**árvore de ataque**) antes de cada exposição ou atividade importante da instituição, especialmente as polêmicas que possam envolver protestos, vandalismos ou outros riscos associados.

Inspecionar fisicamente os equipamentos para verificar se não houve instalações de hardware não autorizadas. Limitar a instalação de novos softwares e hardwares aos administradores.

Prever possíveis desastres naturais que possam impactar a integridade dos dispositivos eletrônicos e dos seus backups. Por exemplo, instituições sujeitas a enchentes podem ter seus primeiros andares alagados. Portanto, é preciso armazenar backups e equipamentos importantes nos andares superiores.

Manter uma caixa física para coleta de bilhetes anônimos ou um formulário eletrônico também anônimo nos quais os funcionários ou qualquer outra pessoa possam fazer denúncias relativas à violação de cibersegurança, comportamentos negligentes dos funcionários, falhas detectadas nos sistemas etc. Educar a equipe de que denunciar não é ser “dedo-duro” e sim responsável para com a função social da instituição.

Adotar o uso de um serviço **VPN** (*Virtual Private Network*), que encripta as comunicações na Web, garantindo que não sejam interceptadas e interpretadas no caminho. Não confiar em serviços

gratuitos. Utilizamos McAfee e Proton.

Plano Diretor da GLAM – Subitem Cibersegurança

Ao elaborar o Plano Diretor, Plano Estratégico ou Plano Museológico da GLAM, incluir um subitem dedicado à cibersegurança, com as seguintes providências previstas:

Identificar informações e sistemas a serem protegidos.

Estruturar a gestão das rotinas e projetos em softwares gerenciais seguros. (Planejamento de empréstimos e exposições, por exemplo, podem ser utilizados para organizar golpes ou roubos.)

Categorizar sistemas (por vulnerabilidade, risco, impacto se crackeado, sigilo etc.).

Identificar e classificar ativos de informação e dados da instituição (quais informações valiosas precisam ser protegidas de cibercriminosos).

Atribuir corretamente os usuários (responsabilidades, acessos, funções etc.).

Mapear possíveis entradas e pontos de crackeamento (árvore de ataque, modelagem de ameaças).

Treinar a equipe da instituição, consultores, prestadores de serviços e empresas parceiras.

Identificar recursos disponíveis que possam ser aplicados na cibersegurança (humanos, infraestrutura, financeiros etc.).

Estabelecer protocolos de segurança (criptografia de mensagens, manutenção e atualização de softwares e hardwares, acompanhamento de visitantes externos, política de destruição de dados e descarte de equipamentos etc.).

Estabelecer plano de resposta à incidentes de segurança, contingência e gestão de crises, para lidar com possíveis hackeamentos e vazamentos de dados.

Estabelecer um plano de resposta a quedas prolongadas de energia elétrica, internet e/ou comunicação telefônica. Apagões de grande porte podem acontecer por ciberterrorismo ou desastres climáticos. Nestes casos, é preciso prever incremento da segurança humana na instituição, alternância de visitas presenciais entre os membros da equipe e um quadro analógico (post its) onde as pessoas que estiveram no museu podem deixar recados e informações para os

demais que chegarem, dentre outras providências. Veja mais sobre isto adiante neste manual.

Estabelecer um plano de Auditoria de Segurança: revisão periódica do Plano de Segurança vigente, sua eficácia, aplicabilidade e resultados obtidos desde a última auditoria.

Estabelecer um plano de Hackeamento Ético: Prever sistemas a serem testados (incluir parceiros, fabricantes e redes de visitantes), os riscos envolvidos nos testes, o cronograma, os treinamentos prévios, os procedimentos para relatório e comunicação das vulnerabilidades detectadas, bem como os próximos passos necessários para executar medidas defensivas.

Procedimentos Avançados

Caso a instituição possua mais recursos financeiros e de pessoal, procedimentos avançados como os sugeridos nesta seção podem ampliar a segurança física e cibernética da GLAM.

Mapeamento dos rastros da instituição na Internet (***Footprinting***): Identificação das informações públicas disponíveis sobre a instituição, seus softwares e websites.

Pesquisar em:

- Mecanismos de busca e redes sociais.
- Informações do website nos mecanismos de busca e redes sociais.
- Dados disponíveis em relatórios públicos de agências de fomento, sindicatos, associações profissionais etc.
- Dados disponíveis na Dark Web e dados vazados em hackeamentos.
- Indução de erros para análise das mensagens automáticas geradas pelo website etc.

Aderir a sistemas de pagamento seguro para transferências e doações, bem como para pagamentos em lojas on-line ou compra de ingressos on-line no site da instituição.

Mapeamento de Vulnerabilidades: Rastrear sistemas em busca de falhas e brechas de cibersegurança. Comunicar ao público e imprensa acerca de vulnerabilidades descobertas em softwares e sistemas somente após serem corrigidas pelo fabricante ou instituição.

Simular ataques ao museu para analisar o comportamento da equipe e reação aos ataques, envolvendo intrusão no sistema (sem danos, apenas invasão), testes de comportamento (ex: *phishing*) e, ainda, tentativas de golpes (engenharia social).

Contratar um Seguro que cubra acidentes e problemas com cibersegurança, com apólice que contemple os profissionais, a instituição e possíveis indenizações.

FAQ – Perguntas e Respostas para Gestores de GLAM

Público-alvo

Qualquer pessoa conectada à Web se beneficiará da quase totalidade deste FAQ, ainda que tenha sido desenvolvido com foco em gestores e profissionais de unidades de informação e cultura GLAM (Museus, Bibliotecas, Arquivos e Galerias).

FAQ – *Frequently Asked Questions*

Por que cibersegurança é tão importante para as GLAMs?

A cibersegurança consiste em parte fundamental da salvaguarda do acervo de uma GLAM (museu, biblioteca, arquivo ou galeria). Instituições GLAM podem sofrer com ataques cibernéticos, incêndios, enchentes, vandalismos etc. Ter uma forma de recuperar a informação sobre o acervo da GLAM é, também, cumprir a sua missão de salvaguarda.

Dados digitais e informações on-line sobre as GLAMs podem ser utilizadas para toda sorte de golpes, que podem ser aplicados contra a instituição, seus funcionários, voluntários, doadores ou visitantes.

Além disto, é muito mais fácil assaltar um museu ou uma biblioteca do que um banco. Mas estas instituições podem conter bens de alto valor monetário. E informações sobre o acervo, publicadas em repositórios digitais (coleções on-line) ou redes sociais servem de mapa para ladrões de golpistas.

Um dos comércios mais lucrativos do mundo é o de bens culturais e obras de arte. A arte também é uma perfeita forma para se "lavar dinheiro". Deste modo, museus estão vulneráveis a fazerem parte de algo ilegal não somente através de ladrões e hackers, mas também de "respeitáveis" curadores, experts e patrocinadores.

Uma instituição GLAM não pode considerar sua função social plenamente desempenhada se não propicia **estabilidade cibernética** em seus sistemas e instalações. A Comissão Global sobre Estabilidade do Ciberespaço (GCSC), reunida em Paris, definiu "estabilidade cibernética" como sendo "*condição na qual indivíduos e instituições podem estar razoavelmente confiantes em sua capacidade de usar serviços cibernéticos com segurança*".

Qualquer instituição ou blog corre o risco de ser hackeado? Somente websites de instituições GLAM de maior porte correm riscos cibernéticos?

A maioria dos ataques externos são randômicos, não direcionados, realizados por robôs, portanto, visam websites indistintamente. Neste sentido, qualquer website pode ser atacado.

Contudo, grande parte das vulnerabilidades de segurança cibernética partem de **ameaças internas**, ou seja, de pessoas de dentro das instituições e empresas que abusam se seus privilégios ou ampliam o seu acesso por meio de **engenharia social** (táticas para enganar pessoas), visando desde vingança até roubo.

Por que alguém hackearia um website de museu, biblioteca, arquivo, galeria ou instituição cultural? Qual o lucro que alguém poderia obter com esta invasão?

As razões para os ataques cibernéticos às GLAMs vão desde o simples divertimento até a obtenção de lucro, que podem ser altíssimos. O *cracker* pode utilizar da boa reputação do website para melhorar o ranqueamento de outros sites (inserindo *backlinks*), adicionar conteúdo ilegal (pornografia, venda de drogas etc.), coletar e explorar dados dos seus usuários e patrocinadores, encaminhar *spams* pelo site (***spamvertize***), espionar as atividades da instituição e/ou empresas mantenedoras, atacar outros websites via website do museu.

Com informações armazenadas em sistemas de gestão de coleções, invasores podem **planejar roubos presenciais** nas galerias, bibliotecas ou reservas técnicas, com os dados de localização e movimentação do acervo. Ou mesmo na coleção principal, identificando cronogramas de conservação e rotinas dos funcionários. O mercado ilegal de obras de arte, livros raros e documentos históricos é um dos mais lucrativos do mundo. E é muito mais fácil roubar um museu ou uma biblioteca do que um banco.

O ataque pode ser, ainda, para tirar o website do ar como forma de retaliação – **hacktivismo antiético** (por exemplo, por causa de alguma exposição polêmica). Neste último caso, um ataque poderá desfigurar o conteúdo on-line do website (***defacement***) ou deixar o acesso lento, comprometendo a ampla propagação de notas oficiais da instituição no combate às *fake news*.

O website da instituição é um canal de comunicação, mas também de construção de autoridade institucional. E as GLAMs costumam ter grande autoridade, além de salvaguardarem acervos de alto valor histórico e monetário. Ciberinimigos podem invadir um website institucional para se **vingar** de alguém ou para **minar a imagem pública** de uma GLAM.

GLAMs com recursos digitais registram, ainda, dados sensíveis de seus visitantes. Alguns museus

possuem jogos e desafios e armazenam estes dados vinculados ao e-mail e/ou rede social do usuário. Alguns destes jogos coletam dados de comportamento e saúde dos participantes. Outros, sobre meio ambiente e pegadas ecológicas, pedem informações que revelam o padrão de consumo, tais como quantas viagens de avião o visitante realiza por ano, quantas TVs, geladeiras, carros etc. possui em sua residência. E assim por diante.

Por fim, GLAMs que possuem lojas, físicas ou on-line, coletam **dados financeiros** relevantes (compras, contas bancárias, cartões de crédito etc.). Associação de Amigos da GLAM que aceitam doações monetárias também.

Por todos estes motivos, cibersegurança é um ponto extremamente importante para as GLAMs, independentemente do seu porte. Websites hackeados resultam em **perdas de custos de oportunidades** (por exemplo, vendas de ingressos interrompidas), prejuízos diversos (processos legais, perda de propriedade intelectual etc.) e, principalmente, danos à reputação e autoridade institucional.

Leis Gerais de Proteção de Dados, como a LGPD no Brasil e a GDPR na União Europeia, geralmente responsabilizam legalmente as GLAMs por possíveis problemas de segurança cibernética causados aos usuários ou visitantes dos seus websites. Portanto, cibersegurança é uma obrigação ética e legal.

Como saber se o website ou repositório digital foi hackeado?

Algumas vezes os ataques aos websites são bem óbvios, como páginas desfiguradas ou fora do ar.

Entretanto, nem sempre o ataque pode ser facilmente descoberto. Verifique se um ou mais itens a seguir estão acontecendo de forma persistente:

- Alteração brusca na velocidade de carregamento das páginas. O website pode estar sofrendo um ataque **DoS (*Denial of Service*)** ou um ataque coordenado com vários computadores ao mesmo tempo **DDoS (*Distributed Denial of Service*)**. Estes ataques não visam a invasão do computador ou aplicação, mas sua sobrecarga, tirando o website ou serviço “do ar” ou tornando-o ineficiente, lento.
- Mudanças bruscas nas estatísticas do website.
- O Gerenciador de Tarefas do Windows não abre ou não roda corretamente.
- O dispositivo encaminha ou recebe e-mails estranhos, principalmente se isto acontece automaticamente.
- Ao buscar no Google o próprio website (digite no campo de busca site: http://seudomínio.com.br), aparecem poucos (ou nenhum) resultados, metadados incorretos e/ou uma marcação de “site inseguro”.

- A página de login não está funcionando ou está indisponível.
- O website está redirecionando para outro website.
- Aparecem conteúdos estranhos, especialmente links.

Qualquer anormalidade no funcionamento do website ou dispositivo deve ser observada e acompanhada com atenção.

Por que é muito importante checar as pessoas que trabalham na GLAM?

A grande maioria dos problemas causados com invasões e vazamentos ilegais têm sua origem em usuários maliciosos com entrada legítima e autorizada nas instituições e seus sistemas.

Ou seja, funcionários, estagiários e pessoal terceirizado que abusam de seus privilégios ou utilizam engenharia social para ampliá-los de forma desonesta.

Portanto, a checagem do passado e acompanhamento do comportamento dos funcionários, estagiários e parceiros da instituição é imprescindível para garantir a cibersegurança da instituição.

Por que não devemos utilizar redes sociais comerciais (exemplo: grupos de Facebook) para gerir a comunicação interna da equipe da GLAM?

Redes sociais comerciais possuem regras próprias e podem alterá-las a qualquer momento, inclusive removendo páginas, grupos e perfis sem dar qualquer explicação aos usuários. Construir sua comunicação, bem como o *marketing* institucional, com base em redes sociais é como construir sua casa em um terreno alugado.

Além da coleta dos dados e do uso de anúncios, que distraem e comprometem a privacidade dos usuários, as redes sociais comerciais são regidas por algoritmos, ou seja, não há garantia de que a equipe vá receber os posts publicados pela instituição nas páginas e grupos.

De preferência, instale intranet e/ou rede social própria no website do museu, livre de algoritmos, coletas de dados, anúncios e outras interferências no processo de comunicação.

É possível construir uma intranet e rede social própria com o WordPress com os plugins BuddyPress e bbPress. Com estas extensões a GLAM pode desenvolver sua própria intranet, rede social, fóruns e todos os recursos disponíveis nas redes sociais comerciais, com a vantagem de que a instituição terá total controle sobre estes canais.

Existem, ainda, inúmeros softwares de gestão bem mais eficientes do que as redes sociais, tais como Basecamp, Taiga e Todoist.

Infelizmente, as instituições hoje em dia precisam estar nas redes sociais. Mas estas não devem ser um local de gerenciamento de equipe ou a principal forma de se conectar com os visitantes. Pesquisas mostram que o retorno de investimento e o engajamento com as newsletters é maior do que com as redes sociais. Utilizamos o software de gestão de *mailing* Brevo para newsletters.

O que é Mapeamento de Risco (árvore de ataque) de uma exposição, evento ou ação da GLAM?

Mapeamento de Riscos (árvore de ataque) é a tentativa de antecipar possíveis ataques que venham a ser realizados contra o website e redes sociais da instituição.

Antes de cada ação, projeto ou exposição, especialmente as polêmicas, identificar possíveis perfis de **hacktivistas** ou **ciberterroristas** que poderiam atuar naquela causa temática, procurando prever suas ações e motivações implícitas: vingança, chantagem, raiva, vandalismo, espionagem, divergência intolerante de pensamento etc. Supor quem, por que, quando, como e onde (quais sistemas e aplicativos seriam atacados).

Procurar supor, ainda, possíveis *fake news* associadas à exposição, deixando pronto materiais de combate às notícias falsas (notas oficiais de esclarecimento, catálogo do conteúdo exposto, sinalização de faixa etária recomendada aos visitantes etc.). A prevenção é sempre a melhor opção.

Cibersegurança dos Websites e Repositórios Digitais

Público-alvo

Qualquer Desenvolvedor Web se beneficiará da quase totalidade desta seção do manual, ainda que tenha sido desenvolvida para *web designers*, *webmasters* e profissionais de unidades de informação e cultura GLAM (museus, bibliotecas, arquivos e galerias).

O que é o WordPress?

O **WordPress** (WP) é um CMS (*Content Management System*). Ou seja, um sistema de gestão de conteúdo. Baseado em linguagem PHP, com banco de dados em MySQL, trata-se de um software gratuito e código aberto (*open source*), que permite publicar e gerenciar conteúdos on-line.

Cerca de um terço dos websites da Internet utiliza o WordPress, escolhido por dezenas de milhões de pessoas no mundo.

O que é o Tainacan?

O **Tainacan** é uma plataforma gratuita e código aberto que permite o desenvolvimento de repositórios digitais profissionais no WordPress, por meio de plugins e temas.

Em termos leigos, um **plugin** é um pequeno programa que se acopla a um software principal para acrescentar funções que este software normalmente não tem. A maioria dos websites não precisa de um repositório. Por isso, o WordPress, por padrão (instalação *core*), não tem esta função. Mas "encaixando" o Tainacan no WordPress, podemos criar repositórios completos, como uma biblioteca ou arquivo digital, uma coleção on-line ou um museu virtual.

Já um **tema** é um *template*, um modelo que possui recursos e formatos prontos para a construção de websites e de coleções on-line.

Simplificando um pouco, porque um tema de WordPress pode ir bem mais além do que a simples aparência, o tema do Tainacan nos fornece um padrão no qual podemos inserir a nossa coleção de modo com que ela fique funcional e bonita, assim como um *template* do Power Point ou do Canva nos ajuda a construir uma apresentação melhor.

O WordPress e o Tainacan são seguros?

O WordPress é altamente seguro, especialmente sua instalação padrão (*core*).

Analisando a lista CVE de vulnerabilidades e exposições do WordPress, mantida pelas agências de cibersegurança dos EUA, notamos que, em grande parte, a maioria das falhas do gênero afetaram plugins e temas, não o *core* do WordPress.

Diversos museus, bibliotecas, arquivos, universidades, veículos de imprensa e instituições culturais confiaram no WordPress para publicar seus websites.

São alguns exemplos: Collections Trust (responsável pelo padrão Spectrum para gestão de coleções do Reino Unido), Guggenheim Foundation (Museus Guggenheim), Escola de Design de Harvard, ICOM – International Council of Museums, O Instituto de Internet da Universidade de Oxford, website oficial da Casa Branca do governo dos EUA.

O WordPress, assim como o Tainacan, procura sempre corrigir suas falhas de segurança de modo rápido e eficiente, lançando novas versões sempre que alguma vulnerabilidade é detectada. Além disto, diversos plugins com versões gratuitas, como os plugins da Wordfence, fortalecem a segurança do WordPress e do Tainacan.

Justamente por ser largamente utilizado, respondendo por cerca de um terço de toda a Web, o WordPress é também extremamente visado pelos cibercriminosos, bem como ataques aos seus websites acabam recebendo maior atenção da mídia.

Cibersegurança faz parte da salvaguarda do acervo das GLAMs. Nenhum website do mundo é 100% seguro. Quando se trata da Web, o objetivo é reduzir riscos e não eliminar riscos. Entretanto, seguindo os procedimentos recomendados e adotados por este manual, as chances de hackeamento reduzem drasticamente.

Plano de Segurança para Websites, Repositórios Digitais e Arquivos Eletrônicos da GLAM

Plano de Backups

Instalar um plugin de backups no website WordPress e realizar o backup de acordo com a frequência de atualização do website (backups de 4 em 4 horas, diariamente, semanalmente, mensalmente etc.). Utilizamos **UpdraftPlus** e backup com Softaculous.

Manter ao menos 3 versões (**backups redundantes**) dos websites e repositórios digitais da instituição. Estes backups devem ser armazenados em meios e localidades diferentes. Por exemplo: um na nuvem criptografada, um no museu em um HD externo criptografado e outro HD em instituição parceira, igualmente criptografado.

A instituição parceira não deve se localizar próximo ao edifício da instituição original, porque em caso de desastres naturais, ambas poderiam ser atingidas da mesma forma. Alguns plugins de backup permitem salvar automaticamente uma cópia em um armazenamento remoto. Escolha um serviço seguro e criptografado, protegido por senha forte.

Verificar se a mídia do backup não está obsoleta (não existe mais equipamento na instituição para acessá-la) ou se não degradou. CDs, por exemplo, envelhecem e se tornam inacessíveis com o tempo ou mediante armazenamento precário.

Periodicamente **testar um backup**, conferindo os arquivos salvos nele ou recriando o website em uma nova instalação utilizando somente o backup.

Guardar os backups antigos, para restauração do website hackeado. Em caso de demora na detecção de um ataque, os backups recentes podem estar contaminados. Portanto, faça novos backups, mas não delete todos os antigos.

Conhecer previamente os procedimentos de backup e recuperação de websites hackeados da sua empresa de hospedagem (Plano de Gestão de Crises a seguir neste manual).

Plano de Auditoria

Acessar o website diariamente e conferir *front-end* (website para visitantes) e *back-end* (atualizações disponíveis, estatísticas do tráfego, intranet etc.).

Procurar o website periodicamente no Google e demais mecanismos de buscas, observando conteúdos estranhos e sinalizações dos buscadores.

Escanear com regularidade o website em ferramentas de detecção de problemas.

Instalar um plugin de monitoramento de logins e atividades no website e repositório, quando forem utilizados por mais de um funcionário.

Consultar regularmente a versão em inglês do Codex do WordPress em busca de novidades, pois as versões em português se encontram frequentemente desatualizadas.

Caso haja orçamento, contratar checagens, auditorias e testes externos (hackeamento ético) do website da instituição, para verificação de suas rotinas de segurança.

Gestão de Crises: Plano de resposta à incidentes de segurança

Manter a calma e não postar detalhes ou opiniões nas redes sociais até ter certeza do que está acontecendo. Caso o hackeamento tenha se tornado público, avisar nos diversos canais de comunicação que estão cientes do problema e trabalhando em uma solução.

Entrar em contato imediatamente com a empresa de hospedagem.

Acionar o seguro, caso possua um que cubra ataques à websites.

Redirecionar o website para uma página html de manutenção (ter esta página pronta para emergências), evitando com isto prejuízo no ranqueamento dos mecanismos de busca.

Documentar em um diário o que está acontecendo, quais mudanças recentes no website foram feitas (exemplo: plugins instalados etc.), horário de detecção do hackeamento, dentre outros dados úteis para análises posteriores.

Baixar o *Raw Access Logs* no cPanel, para futura autópsia do hackeamento.

Escanear o(s) computador(es) de acesso aos websites com um antivírus atualizado.

Fazer um backup do website hackeado, para análises futuras do que aconteceu. (Cuidado para não sobrescrever backups sadios anteriores). Salvar este backup contaminado em uma mídia separada.

Restaurar um backup anterior ao hackeamento. Se a perda de conteúdo for muito grande, considerar a contratação de um especialista em segurança para tentar remover o hackeamento,

mantendo o website íntegro. Mas em tese, se a instituição mantém um cronograma rigoroso de backups, na maioria dos casos será possível recuperar um backup sadio sem grandes perdas.

Após análise forense do backup hackeado, consertar as possíveis vulnerabilidades identificadas. Comunicar todos os envolvidos nestas vulnerabilidades: usuários, desenvolvedores Web, plugins envolvidos etc.

Remover o website hackeado de listas "negras" dos mecanismos de busca, como Google e Bing. (Obs: "lista negra" ou "*blacklists*" é um racismo estrutural da língua portuguesa e inglesa, mas infelizmente é o termo ainda é o mais comum na língua inglesa).

Alterar todas as senhas de todos os usuários (painel WP, cPanel, sFTP, e-mails etc.)

Se tiver recursos, contrate uma auditoria de segurança para verificar se todas as vulnerabilidades foram sanadas e identificar o ponto de entrada do cibercriminoso.

Gestão de Usuários

Atribuir corretamente as funções para cada usuário, concedendo-lhes somente o imprescindível para realização de suas atividades nos websites (*Principle of Least Privilege* ou *Principle of Least Authority*).

Nas Configurações do WordPress, desmarcar a opção "qualquer pessoa pode se registrar". Caso o registro automático seja imprescindível, verificar se a função padrão do novo usuário é a "Assinante".

Deletar todas as contas com logins óbvios, como "admin" ou o nome do usuário, especialmente nas contas com função de Administrador ou Super Administrador para instalações Multisite.

Criar uma conta separada para publicação de conteúdo (posts etc.) com a função de "Editor", evitando acessar a conta de Administrador em computadores e dispositivos externos à instituição ou residência.

No perfil dos usuários, acrescentar "apelidos" (nome do usuário) e selecionar um nome de publicação diferente do login.

Retornar usuários para perfis mais restritivos sempre que se encerrarem trabalhos temporários que exigiam a liberação de funções avançadas.

Deletar usuários inativos ou alterar suas permissões para "Assinante".

Monitorar os comentários, desabilitando-os sempre que não forem imprescindíveis. Caso sejam imprescindíveis, exigir o preenchimento de nome e e-mail, bem como aprovar os comentários manualmente, um por um.

Se forem poucos os comentários do website e permitirem uma investigação mais atenciosa, verificar as credenciais do autor um por um antes de publicar (e-mail válido, contas de redes sociais ativas etc.)

Desabilitar *pingbacks* e *trackbacks*, pois podem ser entradas para ataques DDoS.

Instalar o plugin antispam Akismet.

Instalar recursos CAPTCHA por meio de plugins ou Cloudflare.

Assinalar comentários com códigos (linguagem de programação) como spam.

Evitar comentários com URLs. Caso autorize a publicação de um comentário com URL, verificar a confiabilidade do endereço. Desconfiar severamente de comentários com mais de uma URL.

Não publicar comentários em línguas desconhecidas.

Fechar comentários de posts “datados” após algumas semanas. Por exemplo: um post de uma exposição ou evento que já se encerrou.

Atualização dos Sistemas

Manter o website sempre com a última versão do WordPress, temas e plugins. Explorar softwares, plugins e temas desatualizados consiste na forma mais comum de invasão de websites. Não há como garantir a segurança de um website que esteja desatualizado, pois a cada nova versão lançada, não somente os erros de segurança são corrigidos, mas também informados ao público. Ou seja, um invasor fica totalmente ciente das fragilidades existentes nas versões antigas e pode explorá-las livremente.

Sempre que possível, ativar atualização automática e/ou habilitar alertas para a existência de novas versões do WP, temas e plugins. Toda atualização pode provocar danos ou incompatibilidades no WP, mas vale a pena o risco pelo incremento da segurança. É só conferir os websites com frequência para verificar se está tudo certo.

Deletar temas e plugins desativados. Manter somente aqueles recursos mais necessários, de uso constante. Nada que não esteja sendo utilizado deve permanecer na instalação do WordPress. Portanto, delete temas e plugins quando desativá-los. Alguns vírus se instalam no primeiro plugin

desativado que encontram no WordPress, justamente porque ali serão mais dificilmente descobertos, podendo "estragar" o código do plugin e invadir o website sem ser imediatamente notado.

Utilizar conexão criptografada com o servidor ao transferir arquivos para o servidor da instituição ou empresas de hospedagem.

Seleção de extensões: temas, plugins e códigos

Baixar o WordPress, temas e plugins somente de seus respectivos sites oficiais ou do WordPress.org

Utilizar somente softwares, plugins e temas obtidos diretamente de suas fontes oficiais é um passo importante para garantir a segurança do website WordPress. O melhor local para baixar estes recursos é o repositório oficial do WordPress.org, cujos desenvolvedores estão sempre vigilantes para excluir plugins e temas suspeitos.

Jamais baixe plugins e temas de websites de terceiros ou de repositórios de download, a menos que tenha muita confiança na fonte.

Instalar o mínimo de códigos externos possíveis, como vídeos incorporados e widgets em Javascript. Somente adicionar códigos de fontes confiáveis e checar periodicamente se não houve alterações substanciais no website de onde se extraiu o código, como mudança de proprietário ou nova versão de política de privacidade.

Antes de adicionar qualquer recurso ao WordPress, caso tenha dúvidas se aquela extensão é confiável, verifique se atende aos requisitos abaixo:

- Constar no repositório oficial do WordPress ou em mercados privados tidos como confiáveis pela maioria dos desenvolvedores, como Envato.
- Reputação do desenvolvedor e de outros donos que venham a adquirir o plugin (Em caso de mudança de proprietário, checar credenciais do novo dono, se não foram adicionados conteúdos maliciosos ou mudanças de funcionalidades, política de privacidade etc.). No caso da Envato, dê preferência para os recursos desenvolvidos por "*Power Elite Author*".
- Existência de website oficial e, preferencialmente, contatos físicos dos desenvolvedores. O anonimato, neste caso, não fala a favor do plugin. (Onde se localiza a empresa e por quê?)
- Clareza e profundidade da documentação.
- Existência de *Termos de Serviço e Política de Privacidade*, o que revela profissionalismo e transparência do desenvolvedor. Verificar o que ela coleta e o que compartilha.

- Tempo de experiência do plugin no mercado.
- Data da última atualização e frequência. Não instale ou mantenha plugins que estejam desatualizados há mais de um ano.
- Compatibilidade com a última versão do WordPress.
- Avaliação e comentários de usuários, que devem ser altas e predominantemente positivas. Isto não garante a qualidade de um plugin, pois muitas recomendações podem ser "compradas", tanto as positivas quanto as negativas (concorrência querendo prejudicar a reputação do plugin). Entretanto, um plugin que tenha um número grande de avaliações negativas deve ser analisado com cautela.
- Aceitação Geral: número de instalações ativas (comparar com demais temas e plugins da categoria).

Em caso de dúvida, confira os índices de risco do código do plugin (**Code Risk**), suas estatísticas e ranqueamentos (por exemplo, na plataforma builtwith.com) e/ou analise detalhadamente o código antes de instalar e/ou atualizar.

Testar previamente temas, plugins e códigos em uma instalação de teste ou cópia paralela do website antes de adotá-los nas plataformas oficiais da GLAM. É recomendável manter um *template* pronto para estes testes, contendo todas as configurações básicas de um website, para agilizar este processo.

Não manter arquivos antigos ou temporários em sua instalação WordPress, em especial renomeados com prefixos do tipo "antigo", "old" etc.

É importante, ainda, controlar o acesso às informações e repositórios git de versões em desenvolvimento, não deixando estas versões públicas ou dando acesso às mesmas por pessoas não autorizadas pelo projeto.

Seleção de Empresa de Hospedagem

A escolha de uma empresa de hospedagem consiste em um dos passos mais importantes para garantir a segurança do website. Portanto, seguem-se alguns critérios para nortear esta seleção.

Painel de Controle cPanel

O cPanel consiste em um software de gestão de hospedagem Web utilizado por algumas das principais empresas do ramo. Com ele é possível verificar estatísticas detalhadas dos websites hospedados (exemplo: memória consumida), realizar backups, configurar protocolos de

segurança, instalar softwares em poucos cliques, dentre outras facilidades. Caso sua hospedagem não utilize o cPanel, confira se o painel de controle disponível é seguro e contém todos os recursos do cPanel.

Instaladores automáticos de softwares (*Auto Installer*)

Instalar manualmente softwares, como o WordPress, requer treinamento profissional. Entretanto, quase todas as hospedagens oferecem instaladores automáticos que simplificam este processo. Com estes instaladores, o WordPress pode ser configurado em poucos cliques, quase que automaticamente.

Já instaladores como o Softaculous oferecem o WordPress e outras centenas de aplicações código aberto úteis às GLAMs, tais como Omeka e Moodle. Se a instituição também utilizar estes softwares, verifique se a empresa de hospedagem possui Softaculous ou similares.

Certificado HTTPS (TSL/SSL)

Quando aparece um "cadeadinho" ao lado do endereço de um website no navegador (FireFox, Microsoft Edge, Chrome etc.) ou quando um website possui protocolo HTTPS (a letra "S" após o Http), significa que a comunicação entre o site e o navegador é criptografada.

Verifique se a sua empresa de hospedagem possui algum certificado SSL de criptografia confiável e incluído no seu plano de hospedagem.

Isolamento das contas em servidores compartilhados

Grandes empresas e instituições podem arcar com os custos de servidores exclusivos, ou seja, computadores que armazenam somente dados e websites daquela empresa. Seja localmente, com servidores na empresa ou instituição, seja contratando estes serviços nas empresas de hospedagem.

Contudo, nem sempre uma instituição GLAM poderá suportar estes custos, preferindo hospedar seus websites em empresas que utilizam servidores compartilhados, ou seja, um computador que armazena o conteúdo de vários clientes ao mesmo tempo.

Isto amplia o risco de contaminação, pois caso um website no servidor seja hackeado, os demais que compartilham aquele equipamento também se encontram sob risco. Para minimizar este problema é possível isolar as contas no servidor compartilhado ("*jailed*"). Verifique se sua empresa de hospedagem possui este recurso de isolamento das contas.

Backups automáticos dos últimos 30 dias

Às vezes demora-se alguns dias (ou até semanas) para identificar que um website foi hackeado. Portanto, além de manter backups antigos, é recomendável escolher empresas de hospedagem que realizem backups automaticamente, pelo menos dos últimos trinta dias.

Em caso de uma invasão cujo dano tenha sido irremediável, com o backup é possível deletar o website contaminado e substituí-lo por um backup limpo recente, minimizando as perdas e prejuízos.

Compatibilidade com plugins avançados

Nem toda empresa de hospedagem ou planos mais baratos oferecem compatibilidade com plugins avançados do WordPress, como o WordFence. Em websites profissionais o uso destes plugins é indispensável.

Portanto, antes de contratar um serviço verifique se ele atende aos pré-requisitos necessários de um uso profissional do WordPress.

Recursos de otimização da velocidade e segurança do website

Hospedagens profissionais oferecem recursos adicionais de segurança, bem como de otimização da velocidade de navegação, como CDN e Cloudflare.

A localização dos servidores também pode impactar na segurança e na velocidade, então, verifique em qual localidade a empresa oferece seu data center e escolha uma próxima do seu público-alvo.

Opte, ainda, por servidores localizados em países que ofereçam segurança física e política, cuja democracia seja sólida e não haja guerras em curso.

Atualização automática de versões

Hospedagens profissionais de websites oferecem a possibilidade de configurar diversas atualizações automáticas de versões, como atualizações do WordPress e seus plugins.

Atualizações do *core* podem provocar impactos negativos no website, como rupturas. Além disto, plugins e temas utilizados podem ser incompatíveis com a nova versão do WP. É raro de acontecer, mas dependendo do porte e importância da sua GLAM, é preciso cautela ao ativar instalações

automáticas.

Ao acionar as atualizações automáticas, garanta um plano de backups consistente, para assegurar a recuperação do website em caso de danos extremos.

Em um plano ideal, todas as atualizações seriam feitas diariamente pelo webmaster, conferindo em seguida se está tudo bem com o website. Entretanto, nem sempre isto é possível, por falta de funcionários dedicados na instituição para este fim ou até mesmo férias da pessoa responsável por esta tarefa.

Disponibilização de versão "staging" do website

Hospedagens profissionais oferecem a possibilidade de criar uma versão "*staging*" do website, ou seja, uma cópia do website para atualizações e testes, em paralelo à versão vigente.

Quando a versão *staging* encontra-se apta para ir ao ar, é possível rapidamente substituir o website antigo pelo novo atualizado.

Este recurso pode ser dispensável no caso de websites menos complexos.

Suporte eficiente 24/7/365, em diversas modalidades

Trata-se de um dos principais itens a serem observados na contratação de uma empresa de hospedagem. A empresa deve oferecer suporte 24 horas, 7 dias por semana, 365 dias por ano, em diversas modalidades (telefone, chat, ticket etc.). No caso de empresas estrangeiras, conferir as línguas disponíveis no suporte, de acordo com o perfil da equipe da instituição (muitas disponibilizam suporte somente em inglês).

Opte por empresas cuja equipe de suporte esteja preparada e disposta a solucionar não somente os problemas de hospedagem, mas também dúvidas e dificuldades com o WordPress, pois os limites entre servidor e CMS às vezes são tênues na solução de problemas.

Hospedagem de Websites e Repositórios Digitais

Aviso importante: Antes de começarmos, é importante ressaltar que este projeto não aceita anunciantes ou possui links afiliados. Todas as opiniões abaixo são frutos de nossas pesquisas e experiência técnica de duas décadas gerindo plataformas na Web.

WordPress.com

O **WordPress.com** é uma empresa de hospedagem e serviços baseados em WordPress. Pertence à Automattic, empresa fundada por um dos criadores do software WordPress, o Matt Mullenweg. Hospedar o website na WordPress.com, em geral, implica em anuidades mais caras do que os de uma empresa de hospedagem comum, mas pode ser uma vantagem para os dois extremos.

O primeiro extremo são as empresas e instituições GLAM de grande porte, com muitos recursos, que preferem pagar pelo conforto de um serviço de alta qualidade em WordPress, sem se preocupar com nada relativo à manutenção de servidores e do próprio CMS. Estas empresas contratam os pacotes VIPs de hospedagem, customizados de acordo com a demanda. Grandes empresas, como a Meta do Instagram, são clientes deste serviço.

Já para o outro extremo também pode ser uma vantagem: instituições GLAM muito pequenas ou websites/blogs pessoais, especialmente de usuários que não possuem (e nem querem possuir) muita familiaridade com desenvolvimento Web. No WordPress.com é possível construir um website completo já nos planos mais acessíveis.

O WordPress.com possui planos gratuitos, entretanto, os websites exibem anúncios (que é a forma como a empresa monetiza). Geralmente são propagandas do próprio Wordpress.com. Nos planos gratuitos, não é possível customizar a URL, que será necessariamente nomedomuseu.wordpress.com.

Para fins de pesquisa, nós mantivemos por alguns anos um website no Plano Pessoal, o plano mais barato da WordPress.com. Com este plano, é possível customizar o domínio (nomedomuseu.org ou outra extensão), remover os anúncios (estão presentes no plano gratuito), instalar plugins, dentre outros benefícios.

A experiência com a Wordpress.com foi bem-sucedida. O serviço da WordPress.com nos pareceu simples de usar, eficiente e consistente. Além de ter um excelente serviço de suporte em português.

Empresas de Hospedagem

O WordPress.org possui empresas de hospedagem que são parceiras do projeto. Ou seja, contratando uma dessas empresas de hospedagem via links do website do WordPress, o projeto recebe um percentual (link de afiliados), sem que isto altere o custo do plano para o usuário.

Quando publicamos este manual, as três empresas parceiras do WordPress.org são: Pressable, Bluehost e Hostinger. Destas três, já utilizamos somente a **Hostinger** em um website. Foi uma experiência positiva.

A coordenadora deste projeto hospeda seus websites acadêmicos e pessoais na **FastComet** há alguns anos, também com experiência extremamente positiva. Optamos por hospedar nossas principais plataformas em um servidor localizado na cidade de Londres, mas a FastComet possui servidor também em São Paulo - Brasil. A empresa atende a todos os requisitos listados neste manual, mas o suporte é em inglês.

Para instituições com acesso a profissionais de TI, uma opção viável de qualidade é a **Digital Ocean**, provedora de infraestrutura em nuvem norte-americana, que disponibiliza planos para todos os orçamentos, em geral com maior custo-benefício do que as empresas convencionais de hospedagem. Contudo, nestes casos, além dos websites, será necessário instalar e gerir os softwares do servidor.

É uma empresa altamente recomendada por inúmeros desenvolvedores Web que conhecemos ou que atuam na mídia especializada, tendo a Digital Ocean alguns clientes importantes ao redor do mundo. Contudo, como o foco das nossas pesquisas é WordPress e *Front-End*, optamos por uma empresa que faça por nós o gerenciamento dos servidores. Para instituições GLAM com orçamento permanente de manutenção ou com profissionais de TI na casa, contratar empresas de infraestrutura em nuvem pode significar maior controle e menor custo.

Servidores Institucionais

Este item foi extraído do artigo Gestão Inclusiva e Acessibilidade nos Repositórios Digitais: A Experiência do LavMUSEU, Webmuseu e Tainacan Lab ECI UFMG, de autoria da coordenadora deste projeto. O texto foi atualizado e adaptado para este manual.

As principais vantagens de se optar pelos servidores da própria GLAM são a plena institucionalização do website e a total gratuidade, já que a partir de então o projeto não teria que custear empresa de hospedagem. Desde modo, utilizando infraestrutura própria, o WordPress/Tainacan consiste em uma plataforma 100% gratuita. Isto é importante em termos de sustentabilidade econômica.

Além disto, uma outra vantagem consiste no fato de que o suporte da TI auxilia não somente nas questões de servidor, como é o caso das empresas de hospedagem, mas também nas questões envolvendo o próprio WordPress e Tainacan. Trata-se, portanto, de um suporte de escopo mais ampliado e com interesses mais diretos no sucesso do website/repositório.

Nas empresas comerciais de hospedagem, não há envolvimento institucional por parte dos funcionários responsáveis pelo suporte, que são sorteados de forma randômica. E nem um suporte que vá para além de questões de servidor.

As principais desvantagens de se utilizar servidores institucionais ou de órgãos públicos geralmente são: as possíveis defasagens tecnológicas por limitações de recursos (verba para novos servidores, recursos humanos reduzidos etc.), o acesso limitado dos administradores dos websites às funcionalidades de servidor, as possíveis fragilidades de cibersegurança e o suporte técnico em horário limitado. Explicamos melhor estes pontos a seguir.

Nem sempre as instituições, especialmente as públicas, mantêm seus servidores com softwares e linguagens de programação tão atualizadas quanto as empresas comerciais. Isto pode gerar impacto na cibersegurança e, ainda, no funcionamento do website.

Justamente por questões de segurança cibernética, a equipe de TI da instituição nem sempre fornece acesso amplo e irrestrito às funcionalidades associadas ao servidor, tais como códigos e instalações do WordPress.

Vejamos um exemplo comparativo. Na FastComet, a autora deste manual tem acesso irrestrito ao cPanel e seus recursos. Já no Tainacan Lab ECI UFMG, instalado nos servidores locais da ECI, todas as ações em nível de servidor, backup, novas instalações de WordPress etc. precisam ser mediadas e realizadas via equipe de TI da instituição. O que é uma medida necessária para proteger a instituição de ataques hacker.

Por fim, os funcionários da TI das universidades e GLAMs trabalham somente em horário comercial e com fila de espera para atendimento. Enquanto empresas de hospedagem fornecem suporte 24 horas por dia, 7 dias por semana, 365 dias por ano, com tempo médio de resposta que podem ser de minutos, para os casos mais graves, a poucas horas, para dúvidas e problemas mais triviais.

Portanto, decidir entre uma empresa de hospedagem e um servidor institucional é algo que envolve avaliar criteriosamente qual infraestrutura a GLAM realmente tem à sua disposição em termos de TI. E, também, envolve as formas de pagamento e contratação destas empresas, já que tudo no serviço público costuma requerer licitações e processos burocráticos.

FAQ – Perguntas e Respostas do Desenvolvedor Web

Não tenho condições de manter protocolos sofisticados de cibersegurança nos websites e repositórios digitais da nossa GLAM. Quais destes procedimentos são totalmente imprescindíveis?

Caso não seja possível seguir na íntegra os protocolos recomendados neste manual, adote ao menos os procedimentos de segurança a seguir, que serão eficazes na contenção da maioria das vulnerabilidades:

- Usar logins pouco óbvios e senhas fortes.
- Conceder função de administrador somente quando imprescindível, limitando ao máximo o número de usuários do website. Criar uma conta de "Editor" para atualizações do website.
- Escolher bem a empresa de hospedagem, seguindo as recomendações do manual e demandas da instituição.
- Escolher temas e plugins de confiança, instalando somente aqueles imprescindíveis e deletando os que não estiverem em uso.
- Manter tudo sempre atualizado: WordPress, temas, plugins, bem como os softwares do seu próprio computador.
- Instalar um excelente antivírus no seu computador e mantê-lo sempre atualizado. Recomendamos McAfee.
- Instalar os plugins Wordfence e configurá-los para limitar várias tentativas de login.
- Instalar o UpdraftPlus ou outro plugin de backup, mantendo sempre cópias físicas deste backup na instituição e fora dela.

Alguns procedimentos comuns de cibersegurança de websites, como bloqueio de acessos vindos de certos países, não estão listados neste manual. Por quê?

Ataques de força bruta parecem vir em sua maioria de determinados países. Por isto, muitos desenvolvedores optam por bloquear o acesso destes países aos websites, eliminando grande parte dos problemas.

No caso das GLAMs, que precisam garantir ampla acessibilidade para cumprir sua função social, esta atitude drástica não é recomendada, pois a questão da isonomia de acesso não estaria plenamente contemplada com este bloqueio.

Outro procedimento comum é tentar impedir a navegação ou descobrir os dados de quem navega

no website de forma anônima. Contudo, as GLAMs têm a obrigação ética de levar o conhecimento a todos, o que incluem pessoas bem-intencionadas que podem estar acessando anonimamente o website de países não-democráticos, simplesmente para se instruir.

Isto é especialmente importante no caso, por exemplo, de museus que tratam de temas sensíveis, como holocausto, inquisição, refugiados, meio ambiente e direitos humanos.

Portanto, nenhuma forma de bloqueio de usuários anônimos ou de países específicos devem ser implementados em websites e repositórios digitais das GLAMs. Muitas vezes as equipes de TI fazem isso sem os gestores da instituição saberem, portanto, é importante conversar sobre isto com a equipe que dá suporte tecnológico à GLAM.

Quais as formas de hackeamento mais comuns em websites WordPress?

As formas de ataque mais comuns aos websites WordPress incluem o envio de pedidos HTTP para o servidor, explorando vulnerabilidades como plugins e temas desatualizados, bem como o ataque de força bruta, que utiliza um robô para tentar adivinhar login e senha dos usuários, especialmente dos administradores.

Ataques de força bruta, contudo, não são as formas principais de hackeamento bem-sucedido de websites em WordPress, mas sim a existência de vulnerabilidades no *core* (instalação padrão) do WordPress, temas e plugins. Por isto, mantenha tudo sempre atualizado.

Adotar os recursos de cibersegurança sugeridos neste manual não torna o website da GLAM mais vulnerável, já que todos saberão quais procedimentos adotamos?

Raramente isto faz diferença. Tendo em vista que a quase totalidade dos ataques acontecem por robôs e, portanto, atacam websites indistintamente, a adoção destes recursos aqui propostos é uma informação que um *bot*, por não ser humano, não terá.

Entretanto, se o cibercriminoso estiver promovendo um ataque direcionado a uma instituição específica, quanto mais informações obtiver sobre o website, melhor (para o invasor). Neste sentido, divulgar publicamente a adoção destes ou de qualquer recurso (temas, plugins, empresas de segurança contratadas etc.) facilita, sim, a vida dos criminosos.

Contudo, tenha em mente que “segurança por obscuridade” (próxima questão deste FAQ) é extremamente frágil e ineficaz. É por isto que muitas instituições anunciam em seus blogs a adoção do WordPress ou a contratação de um serviço específico sem grandes reservas.

O que é segurança por obscuridade e por que ela não é recomendada neste manual?

Segurança por obscuridade é uma estratégia primária e pouco eficaz, que consiste em tentar esconder dados de um invasor, para dificultar a invasão. Estes dados podem ser a versão do WordPress, a página de login etc.

O fato é que um invasor experiente e obstinado descobrirá isto e muito mais coisas a respeito do seu website com grande facilidade e rapidez. Daí a importância de cumprir rígidos protocolos de segurança, ao contrário de tentar esconder aquilo que é tranquilamente revelável por um cibercriminoso em poucas horas de investigação.

Por surtir quase nenhum efeito, caso opte por este caminho, recomendamos somente algumas práticas para obscurecer informações, como deletar arquivos desnecessários de instalação, mover o arquivo wp-config.php um diretório acima, não utilizar logins óbvios (ex: “admin”) ou alterar o table_prefix do banco de dados no momento da instalação. Para bancos existentes, deixe como está, pois pode causar danos à instalação. Jamais realize o procedimento posteriormente, com códigos e plugins para alterar o prefixo.

Como a escolha de um domínio pode impactar a cibersegurança do meu website?

O domínio de um website é o seu endereço, a sua URL. Por exemplo, o domínio da plataforma Webmuseu é webmuseu.org O domínio do website da UFMG é ufmg.br

Muitas instituições GLAM são patrocinadas por empresas bilionárias. E algumas delas colocam o seu nome no museu e, também, na URL. Suponhamos, por exemplo, que um museu sobre meio ambiente seja patrocinado pela empresa de energia sustentável SUSTEC. É comum que a URL do museu seja algo assim:

- museu.sustec.com.br
- museu-sustec.com.br
- sustec.com.br/museu

Empresas sofrem muito mais ataques hacker direcionados do que museus, arquivos e bibliotecas. Um ataque direcionado à empresa SUSTEC pode acabar atacando o website do museu. Neste sentido, tenha em mente de que o museu vai ter que se preocupar com a segurança do seu website no mesmo nível que a empresa.

Uma opção melhor seria comprar um domínio “neutro” para o museu, tais como: museudomeioambiente.com.br Converse com a equipe de TI da empresa antes de escolher o domínio da instituição GLAM e saiba qual é o nível de risco de um ciberataque.

Por que toda instituição GLAM ou projeto de pesquisa deveria pensar duas vezes antes de ter seu próprio website ou repositório digital?

Um aspecto importante que contribui para a fragilidade da segurança cibernética e para o não cumprimento das leis gerais de proteção de dados, como a LGPD no Brasil e a GDPR na União Europeia, consiste na incompreensão das demandas de médio e de longo prazo de uma plataforma digital (repositório digital, website, coleção on-line etc.).

Um projeto ou instituição GLAM pode conter recursos iniciais e bolsistas/estagiários/colaboradores engajados, que se dedicam a desenvolver uma plataforma on-line. Entretanto, quando o financiamento acaba e a pessoa engajada vai embora, sendo substituída por outra que não tem a mesma expertise de informática ou o mesmo engajamento que a anterior, a plataforma on-line fica estagnada.

Esta estagnação compromete a credibilidade acadêmica das universidades e a função social das GLAMs, visto que o conteúdo continua muitas vezes acessível na Web, mas desatualizado e/ou com usabilidade apresentando problemas e erros de navegação. Ou ainda, como acontece em grande parte dos casos, a plataforma "sai do ar". Isto representa um enorme prejuízo para a divulgação do conhecimento produzido pelo projeto, além de um grande desperdício de dinheiro, tempo, infraestrutura e esforços intelectuais.

Um website WordPress ou uma coleção on-line desenvolvida no Tainacan, por exemplo, é como um "organismo vivo", que precisa de manutenção constante para "sobreviver" e para se manter seguro. Isto significa ter alguém permanentemente atualizando as instalações do WordPress e os plugins e temas do Tainacan, checando as configurações de segurança e da hospedagem (servidor onde o WordPress se encontra instalado). Sem mencionarmos o próprio conteúdo, que deve ser constantemente revisto e alimentado.

Se ninguém cuidar diariamente ou, no mínimo, semanalmente, deste repositório digital, não só ele deixará de funcionar plenamente com o tempo, mas como também se tornará um alvo fácil de cibercriminosos e vírus. A desatualização de sistemas, linguagens e softwares é uma das principais causas que comprometem a segurança cibernética.

Portanto, antes de começar um projeto na Web – um repositório digital, coleção on-line, website ou laboratório virtual – a equipe da GLAM ou da universidade deve se perguntar as seguintes questões:

1) Este projeto tem um "pai" ou uma "mãe", ou seja, uma pessoa permanente na instituição, disposta a "adotá-lo" *ad infinitum*?

2) Temos verba permanente para sustentá-lo ao longo do tempo (por exemplo: atualização dos servidores institucionais ou custeio de empresa de hospedagem de websites)?

3) Temos uma equipe preparada e engajada para mantê-lo vivo e seguro?

Se a resposta for “não”, talvez seja melhor repensar a criação da plataforma on-line ou desenvolvê-la em plataformas gratuitas mais simples de utilizar, como o **WordPress.com** para websites ou o **Internet Archive** para repositórios digitais.

No Internet Archive é possível criar coleções on-line sem tantos recursos como o Tainacan, porém totalmente gratuitas, sem demandas técnicas de manutenção e cibersegurança, com curva de aprendizado curta (fácil de inserir conteúdo e atualizá-lo) e com maior probabilidade de permanência no longo prazo.

O Internet Archive é mantido por uma organização sem fins lucrativos desde 1996. Enquanto ele existir, e esperamos que seja para sempre, coleções feitas nele permanecerão on-line sem demanda alguma de custo ou manutenção por parte da equipe da GLAM.

Cibersegurança e Inteligência Artificial nas GLAMs

A IA já está revolucionando o mercado de trabalho dos museus, bibliotecas e arquivos. E o seu desenvolvimento, crescimento e adoção está acontecendo de forma desordenada, desregulamentada, centralizada em meia dúzia de Big Techs e exponencialmente perigosa. Não somente para indivíduos e instituições GLAM, mas para a própria sobrevivência do planeta e da humanidade.

E isto não é uma teoria da conspiração, são apenas fatos bem fáceis de serem compreendidos por quem pesquisa sobre o tema, ou mesmo lê e ouve entrevistas dos maiores especialistas no assunto. Para saber mais acompanhe o trabalho da Associação Internacional para a Inteligência Artificial Segura e Ética.

Vários profissionais renomados saíram dessas Big Techs justamente para denunciar a forma irresponsável com que têm conduzido a IA, que está inclusive por trás dos algoritmos das redes sociais. Ganhadores de prêmios importantes, como o Nobel da Física e Turing (o "Nobel" da computação), estão alertando para o fato de que os perigos existenciais associados à IA são reais. Estes especialistas e acadêmicos, que literalmente colaboraram para o desenvolvimento da IA nas últimas décadas, estão agora alertando para os riscos daquilo que eles próprios criaram.

Muitos críticos da IA são taxados de "alarmistas" por afirmarem o óbvio: o desenvolvimento irresponsável da IA pode ter consequências gravíssimas para a sociedade e para o mundo. Em nossa opinião, quem ignora o fato de que a revolução da IA será exponencialmente maior do que outras que a humanidade já enfrentou (como a Revolução Industrial), ou está desinformado, ou está em negação, ou tem uma agenda oculta para minimizar esta informação (como investimentos em empresas de IA ou contratos – secretos ou explícitos – de patrocínio com aplicativos que utilizam IA).

Estas pessoas inteligentes e cultas que minimizam o impacto e os problemas da IA estão do lado errado da história. Estão vendendo sua reputação, provavelmente na esperança de que não viverão o suficiente para sofrer as piores consequências da adoção em massa desta tecnologia.

Sobre os impactos da IA nos museus e no setor cultural, escrevemos um texto de blog que pode ser acessado clicando aqui.

Estes e futuros textos sobre IA no blog podem ser lidos clicando na tag Inteligência Artificial. Não nos delongaremos neste tema no manual, pois não é o foco principal. Iremos direto para alguns dos desafios de cibersegurança associados à IA.

Grosso modo, a IA consiste na capacidade de um software digital em executar ações solicitadas de forma o mais assertiva possível, mesmo sem familiaridade prévia com aquele contexto em si. Os sistemas de IA analisam grandes bancos de dados, fazem inferência a partir desta análise e

tomam decisões com base nas regras gerais que encontrou no banco. De acordo com o feedback obtido do usuário, a IA pode ir aprimorando a precisão destas regras e afinando a eficiência das tarefas a ela demandadas.

A IA "aprende" e emula o cérebro humano. E à medida que os robôs de IA adquirem inteligência espacial, entrarão também nas searas que envolvem destreza manual, como conservação, manutenção, montagem de exposições etc. Robôs comandados por IAs já são capazes de fazer as unhas (remover cutículas, pintar com esmalte, decorar com decalques etc.) e até realizam cirurgias em humanos! Em breve serão capazes de realizar exames diagnósticos e fazer a manutenção ou o restauro de obras de arte em museus ou livros raros em bibliotecas.

A adoção e difusão da IA está acontecendo de forma tão rápida, que não há como acompanhar este uso com **regulamentação governamental** e nem com **protocolos eficazes de cibersegurança**. Sequer os programadores da IA sabem plenamente como essas redes neurais funcionam e qual o seu real potencial de dano. Se nem os especialistas têm certeza da melhor maneira de garantir a segurança destas IAs, o que dirá de todos nós, meros usuários.

Neste sentido, os cibercriminosos que se utilizam da IA para o mal podem estar anos luz na frente dos especialistas em segurança cibernética que a utilizam para combatê-los. Criminosos não possuem uma bússola moral que os impede de agir.

Tanto especialistas em segurança cibernética, quanto hackers e crackers, passaram a utilizar a **IA como ferramenta**. E esse uso é diverso, indo desde a programação de vírus e quebras de senhas até a previsão de possíveis formas para se invadir um sistema específico.

O *AI Security Institute* do Reino Unido demonstrou em seu relatório no ano passado que os principais modelos comerciais de IA generativa poderiam ser "quebrados" e manipulados para agirem contra suas supostas regras de conduta. Além disto, algumas plataformas de IAs já tiveram problemas sérios com vazamento de dados e conversas de seus usuários.

As IAs também potencializarão ao máximo a *engenharia social*. A IA é capaz de analisar grande bancos de dados sobre uma instituição, encontrar pontos de vulnerabilidade ou redes de conexão entre os funcionários, facilitando a aplicação de **golpes sofisticados**.

O uso das ***deep fakes***, principalmente vídeos e áudios, contribuirão para que mais e mais pessoas sejam enganadas pelos cibercriminosos. Estas *fakes* também podem ser usadas para autenticar biometrias, burlando os sistemas de segurança. Portanto, quanto mais conteúdo com seu rosto e voz você publica na Web, mais exposto está a este tipo de quebra de segurança.

Daí a importância de combinar com as pessoas, tanto da vida privada, quanto da vida profissional, uma "senha" ou pergunta-chave que deverá ser feita para saber se estamos falando mesmo com aquela pessoa e não com uma IA simulando uma videoconferência.

Algumas instituições também se utilizam da IA e técnicas de Deep Fake para criar vídeos educativos. Por exemplo, um museu dedicado a um escritor poderia fazer um vídeo de IA deste escritor convidando as pessoas para visitar as exposições. É antiético criar vídeos de pessoas falecidas sem que elas tenham dado autorização prévia para isto. Isto transforma a imagem daquele escritor em um produto, atribuir a ele falas e pensamentos que não necessariamente condizem com sua personalidade e caráter. Estes vídeos *fakes* de IA também podem causar emoções negativas em seus descendentes.

Como as GLAMs são instituições que prezam pela sua função social, precisamos nos atentar para as normas de **ética digital**. Além disto, a veiculação de vídeos *fake*, mesmo que sinalizados, pode dirimir a confiança da população na credibilidade daquela instituição.

Instituições GLAM também não deveriam aderir à memes e *trends* feitos com IA, pois estas empresas que criam aplicativos de memes com IA (tornar uma criança adulta, um adulto idoso, incluir alguém ou algo na imagem etc.) estão coletando nossos dados e biometria gratuitamente, com nossa autorização (**Informação Pessoalmente Identificável - PII**). E não saberemos o que farão com nossa imagem ou dados

Um outro aspecto importantíssimo é a questão dos **direitos autorais e privacidade de dados**. A IA está aprendendo com o conteúdo que compartilhamos com ela, não apenas nos ajudando a produzi-lo.

Por exemplo, um gestor de museu que utiliza a IA para elaborar ou simplesmente melhorar a gramática de um plano estratégico ou plano museológico para a instituição, corre riscos que não imagina. Além de saber informações confidenciais sobre aquela instituição, detalhadas no plano, a IA também está extraindo ali ideias originais e novas, que poderá utilizar quando for demandada a realizar uma tarefa similar, em qualquer lugar do mundo. Isto ocorre especialmente se a instituição está utilizando uma plataforma de IA “gratuita”, como ChatGPT, DeepSeek, Gemini, Claude etc.

Algumas plataformas de IA afirmam que não aprendem com as conversas privadas de seus usuários. Você acredita nisto? Nós desta pesquisa não acreditamos.

Dependendo da política de privacidade da plataforma, as conversas que temos com a IA podem ser lidas por seres humanos, para melhoria e treinamento do sistema. Portanto, ao **finalizar um chat com a IA, não dê feedback**. Conversas que possuem feedback – tanto positivo, quanto negativo – provavelmente têm maiores chances de serem revisadas por um ser humano. Ainda que as plataformas digam que não informam ao revisor de quem é aquela conversa, às vezes é possível inferir esta informação pelos diálogos.

No caso de pessoas neurodivergentes ou pessoas com deficiência, ou seja, nos casos em que a IA é utilizada como **tecnologia assistiva para inclusão**, a situação se torna ainda mais grave.

Vejamos o exemplo de uma pessoa cega. Ela precisa compartilhar com um app de IA a sua câmera, para que a assistência seja efetiva, resultado em uma profusão de imagens e dados partilhados com aquele aplicativo. Nestes casos, o comprometimento da privacidade provavelmente será muito maior do que o uso da IA por pessoas típicas.

A **ausência de um setor efetivo de recursos humanos** nas instituições está ajudando a promover a transferência para as IAs do papel de psicólogo, psiquiatra, mentor, gestor, amigo, colega de trabalho etc. Na falta de suporte gerencial e emocional, o trabalhador encontra na IA "alguém" que parece sempre o colocar "para cima" (as IAs são programadas para isto) e saber de "tudo" (as IAs fingem muito bem este papel).

As IAs são programadas a responderem de modo com que gostemos da resposta, portanto, o que ela nos diz não é confiável. Elogios, respostas que concordam com o usuário e respostas que parecem verdadeiras são as que recebem melhor feedback e engajam mais. Portanto, as IAs estão sendo treinadas para nos manipularem emocionalmente, não para fornecerem informações corretas e precisas.

Um aspecto pernicioso é que a IA simula brilhantemente a interação com um ser humano. Neste sentido, as pessoas estão compartilhando com os *chatbots* informações extremamente pessoais e buscando neles um apoio "terapêutico" ou uma "mentoria" que não encontram em seus ambientes institucionais. E os conselhos administrados pela IA não só podem estar incorretos, como podem levar à piora da saúde mental do trabalhador e até mesmo a comportamentos temerários ou autodestrutivos. E, ainda, expõem dados privados do funcionário e da sua instituição. A IA é programada para nos "bajular" e concordar conosco o máximo que puder para nos manter engajados na conversa, utilizando os serviços e fornecendo nossos dados.

É importante educar os colaboradores da instituição a não acessarem plataformas de IA quando estiverem sob efeito de **drogas ilícitas ou lícitas**, como álcool ou medicamentos. Porque substâncias que alteram nosso estado de consciência podem "abaixar a guarda" para o que fazemos ou dizemos para a IA, tornando ainda mais comprometedora a interação.

Instituições que adotam agentes de IA, ou seja, que terceirizam para uma IA ações concretas e decisões que antes eram tomadas por humanos, podem se deparar com a terrível realidade de descobrir que **cibercriminosos violaram suas plataformas de IA**. Por exemplo, invadindo o sistema e instruindo a IA não só a realizarem as tarefas para as quais foram planejadas, mas também outras atividades ilícitas "por baixo dos panos", como vazar dados confidenciais para os golpistas.

Criminosos também podem hackear equipamentos **AIot (*Artificial Intelligence of Things*)**, que é a união da IA com o Iot, *Internet das Coisas*. Robôs de limpeza ou equipamentos de monitoramento ambiental podem fornecer desde áudio a fotografias dos objetos e espaços, mapeamento da planta das galerias e reservas técnicas etc. Para citarmos apenas alguns dados que podem ser preciosos aos golpistas.

Nenhuma tecnologia digital trouxe tantos desafios de cibersegurança e privacidade de dados como a Inteligência Artificial (IA). As instituições que levam à sério cibersegurança precisarão adotar uma postura cautelosa na implementação destas ferramentas no ambiente de trabalho da GLAM. Um passo de cada vez, com bastante informação técnica e protocolos éticos de conduta.

A função social da GLAM precisa estar acima do nosso fascínio por esta tecnologia disruptiva que já está moldando, à olhos vistos, um mundo bem diferente daquele que conhecemos.

Privacidade de Dados e Cibersegurança nas GLAMS

Vivemos na era do **capitalismo de vigilância** (ZUBOFF, 2021). Neste modelo econômico, a experiência humana é a matéria-prima gratuita que alimenta o lucro das grandes empresas de tecnologia, as Big Techs. Estas empresas mineram os nossos dados, analisam nossas ações e comportamentos on-line – com frequência sem o nosso consentimento – e, a partir desta coleta invasiva, são capazes de nos influenciar e prever o nosso comportamento futuro. Esses dados são utilizados pelas próprias empresas para nos oferecer anúncios e produtos. Ou são vendidos a terceiros para este mesmo fim.

Outro conceito relevante nesta discussão é o da **economia da atenção**. Nesta maneira de gerenciar a informação, a nossa atenção – ou seja, o tempo que dedicamos a algo – é considerada uma mercadoria. E as Big Techs, portanto, aprenderam a capitalizar a nossa atenção, mantendo-nos por mais tempo possível nas telas, utilizando seus serviços e plataformas.

E como as empresas sabem tudo sobre nós? Como podem nos manipular para comprarmos seus produtos e serviços? Ou para apoiarmos as ideias de seus clientes anunciantes? Através do **monitoramento digital**, vigiando tudo que fazemos nas redes sociais, websites, softwares e aplicativos por meio de *cookies* e outros recursos de identificação e coleta.

"*Não preciso me preocupar com privacidade de dados, pois não tenho nada a esconder.*" Esta é uma alegação bastante comum e equivocada acerca da importância da privacidade de dados. Todos nós precisamos de privacidade, em maior ou menor grau, para garantirmos nossa segurança física e cibernética. Além disto, ninguém está imune à influência. Quanto mais estas empresas sabem sobre nós, mais eficientes são em nos manipularem com seus anúncios pagos.

Quando estes anúncios ajudam a eleger políticos ditatoriais ou quando minimizam os perigos do aquecimento global, estamos colocando as democracias e o futuro da humanidade em risco.

A regulamentação da coleta dos nossos dados pessoais

Tentando minimizar os problemas associados à privacidade de dados após a revolução digital, governos de diversos países ou blocos econômicos e políticos – como a União Europeia – promulgaram leis de proteção de dados. Vejamos duas importantes delas:

A **Lei Geral de Proteção de Dados Pessoais – LGPD**, publicada em 2018, é a regulamentação brasileira sobre tratamento de dados pessoais, que visa proteger a liberdade, intimidade, privacidade e livre desenvolvimento da personalidade da pessoa natural. Também aborda a liberdade de expressão e o direito à informação na economia informacional e digital. Aplica-se

não somente ao digital, mas à proteção de dados como um todo. E envolve tanto os dados da pessoa natural ou física, quanto das instituições e empresas.

A ***General Data Protection Regulation*** **– GDPR** seria a legislação equivalente à LGPD da União Europeia, implementada em 2018. Mesmo empresas e instituições que não pertencem à UE precisam seguir a GDPR, caso ofereçam seus produtos e serviços, ou exibam seus websites, nos territórios destes países europeus. O mesmo se aplica às instituições ou empresas de países estrangeiros que, de algum modo, atuam no Brasil – presencial ou virtualmente.

Nestas legislações, a privacidade deve ser encarada por todos como princípio norteador, dentro dos conceitos de ***privacy by design*** e ***privacy by default***.

As leis gerais de proteção de dados merecem seu próprio manual. Para fins desta publicação, iremos listar os principais documentos que esta lei exige das empresas e instituições, que tem total correlação com a cibersegurança dos nossos dados. Para estar em conformidade com a LGPD e GDPR, as instituições precisam apresentar em seus websites e documentos institucionais os seguintes itens (SERPRO, 2025):

- Diretriz de Segurança Lógica (políticas de senha, sistemas de autenticação de usuário, programa de detecção de vírus);
- Normas de Classificação, Anonimização e Criptografia da Informação;
- Política Corporativa de Governança de Dados;
- Política Corporativa de Segurança da Informação;
- Política Corporativa de Privacidade e Proteção de Dados;
- Plano de Resposta a Incidente e Remediação;
- Plano de Continuidade de Serviços e Negócios;
- Plano de Contingência;
- Plano de Comunicação, Treinamento e Conscientização sobre Segurança da Informação, Privacidade e Proteção de Dados; e
- Programa de Governança em Privacidade e Proteção de Dados.

As instituições e empresas que tiverem seus dados vazados por ataques de criminosos, ou agirem de forma negligente com suas obrigações para com a cibersegurança, podem ser penalizadas com pagamento de multas e indenizações aos usuários afetados.

Todo gestor de GLAM precisa se informar sobre suas obrigações mediante estas leis. E todos nós precisamos ler atentamento os documentos listados acima, pelo menos dos principais serviços que contratamos ou plataformas que utilizamos na Web. Neste link a seguir, você pode acessar como exemplo as políticas de privacidade de dados e termos de uso dos websites acadêmicos e blog de divulgação científica da autora deste manual.

Interrupção da Energia e da Internet devido a Ciberataques ou Desastres Ambientais

Toda a sociedade hoje depende da energia elétrica, comunicação telefônica e Internet para funcionar. Somos extremamente dependentes deste sistema operando, mas ele pode falhar, seja por causa de um ciberataque, seja por questões naturais ou desastres climáticos. Não é uma questão de se, é uma questão de quando.

Portanto, estar preparado para lidar com interrupções (esperamos nós que seja temporária) da energia elétrica e da comunicação digital é fundamental para garantir a segurança das GLAMs.

Plano de Emergências Pessoal do Gestor

Para que o gestor possa se dedicar à instituição que lidera, em meio à uma emergência de "apagão total" (queda da energia elétrica e das comunicações, como telefonia e Internet), ele precisa estar tranquilo de que seus entes queridos estão bem e em segurança.

Por isso, o primeiro passo para garantir a segurança da GLAM é que o gestor tenha garantido a segurança de seus familiares e dependentes. Eis algumas sugestões de providências:

- Conversar com familiares sobre a possibilidade de um apagão de energia e das comunicações, que podem acontecer por razões diversas, inclusive, causas provocadas por acontecimentos naturais. Portanto, caso isto aconteça, o primeiro ponto importante é ficar calmo e agir conforme previamente acordado.
- Explicar para crianças, idosos e outros dependentes que, se isso acontecer, os sinais de trânsito não funcionarão, muita gente irá do trabalho embora para casa e o trânsito ficará muito lento. Poderá haver longa demora para que a pessoa responsável entre em contato. Por exemplo, para que o filho visite o familiar idoso ou para que os pais peguem as crianças na escola. Então, é importante permanecer tranquilo e entender que a longa demora, nestes casos, é simplesmente normal.
- Combinar um ponto de encontro familiar, principalmente se pessoas dependentes ou crianças não estiverem na residência. Por exemplo, caso as crianças estejam passeando com os avós no parque, para onde os avós as levam? Para a casa dos pais? Para a casa deles? Qual é o ponto de encontro familiar onde, em caso de apagão, todos devem se direcionar?
- Caso as pessoas estejam em suas residências e não sejam dependentes, o combinado familiar pode ser permanecer em casa por até dois dias, aguardando o retorno da energia e da comunicação. Se este retorno não acontecer em até dois dias, deixar combinado por escrito quem vai na casa de quem, para não haver desencontro.

- Todas as vezes que alguém sair de casa deve deixar um bilhete em cima da mesa dizendo se está bem ou não, se precisa de algo ou não, onde foi e a expectativa de hora de retorno. Assim, caso um parente vá até a residência de outro, saberá por que não tem ninguém em casa e o que fazer.
- Compartilhar a chave da sua residência e do seu gabinete profissional com pessoas próximas e de confiança.
- Manter uma quantia em espécie em sua residência sempre, porque em emergências como um apagão, cartões de crédito não funcionam e as compras de suprimento precisarão ser feitas em dinheiro.
- Manter um estoque de comida em sua residência que seja suficiente para pelo menos uma semana. Pedir que seus parentes mais próximos façam o mesmo, para que não consumam o seu suprimento.
- Ter um rádio e pilhas novas sempre em sua residência, pois em caso de apagão de energia e comunicação, as principais informações chegarão provavelmente via rádio.
- Ter sempre um arquivo em versão impressa e digital, onde seus parentes possam encontrar as principais informações sobre sua vida digital e profissional (além de pessoal) caso haja uma emergência com você: senhas, localização de objetos preciosos escondidos na casa, para quem repassar arquivos/senhas no seu trabalho na sua ausência etc. Esconder muito bem este material, mas informar as pessoas de confiança mais próximas.

Plano de Emergências da Instituição

Desenvolver um plano para quedas prolongadas de energia elétrica e comunicação telefônica, que considere os seguintes pontos:

- Rotina de segurança física da instituição e conservação preventiva do acervo.
- Escala de permanência dos funcionários na instituição, reforçando a presença física no local e, por consequência, garantindo a segurança das coleções.
- Quadro analógico de comunicação (exemplo: quadro com *post its*) no qual os funcionários deixarão informações importantes e recados uns para os outros, quando tiverem ido à GLAM.
- Salvaguarda e realocação das peças mais preciosas da instituição em um local que tenha as condições de controle ambiental adequadas asseguradas por baterias e geradores.
- Em casos extremos, remoção do acervo mais importante da instituição para um outro local mais seguro e protegido.
- Salvaguarda e/ou remoção dos backups portáteis dos arquivos digitais da instituição. É muito importante que o acesso a estes arquivos não dependa da Internet para funcionarem. Por exemplo, a senha de criptografia de um HD, que geralmente é complexa,

precisa estar disponível em algum lugar que não seja o gerenciador de senhas on-line, porque ele pode estar fora do ar.

- Rotinas e medidas de gestão de crises e proteção de saúde mental da equipe, que certamente estará abalada durante o apagão.

Tecnologias e Ferramentas Recomendadas pelo Projeto

Aviso: Manual Livre de Propagandas ou Patrocínios

Os links deste manual não são de “afiliados”. Não realizamos propagandas remuneradas e nem aceitamos patrocínios de empresas e softwares.

Um dos princípios básicos para se garantir a autonomia intelectual de uma pesquisa acadêmica é limitar as fontes de recursos, especialmente aquelas que geram conflitos de interesses.

Todas as empresas e produtos recomendados neste projeto, listadas aqui neste manual, foram selecionados exclusivamente por seu mérito ou pertinência, sem o fornecimento de qualquer outra forma de benefício aos pesquisadores.

O projeto aceita utilizar versões gratuitas de softwares *freemium* ou licenças educativas desde que isto seja uma política da empresa e não um privilégio específico para determinados pesquisadores ou profissionais.

Decidimos compartilhar os resultados desta demorada investigação e de anos de experiência indicando nominalmente nossas marcas e produtos favoritos. O objetivo é economizar o tempo dos profissionais de GLAM que não são especialistas em TI.

Curadoria hoje é fundamental, numa época na qual estamos soterrados de opções e informações, sem saber como escolher de modo apropriado. Ou seja, faz parte deste projeto tomar decisões difíceis e compartilhá-las com quem tem menos expertise ou recursos, como é o caso dos museus brasileiros, que em sua maioria não possui setor de TI e nem terceiriza estes serviços.

Não há qualquer fidelidade às marcas nos nossos projetos e pesquisas projeto, cujas indicações podem (e provavelmente) sofrerão alterações ao longo do tempo. Acesse sempre o website do nosso projeto em busca de novas versões desta publicação.

Nosso compromisso é com o conhecimento, com a função social das GLAMs e com a sociedade brasileira que custeia os nossos salários.

Se tiver sugestões de outros serviços ou discordar de nossas recomendações, entre em contato conosco. Teremos o maior prazer em ouvi-los!

Temas WordPress

AUTOMATTIC. Disponível em: https://automattic.com/> Acesso em: 02 fev. de 2026.
Temas desenvolvidos pela Automattic, empresa de um dos criadores do WordPress, são confiáveis.

DIVI. Disponível em: <https://www.elegantthemes.com/gallery/divi/> Acesso em: 02 fev. de 2026.

IMPREZA. Disponível em: <https://themeforest.net/item/impreza-retina-responsive-wordpress-theme/6434280> Acesso em: 02 fev. de 2026. Tema preferido pela autora do manual.

TAINACAN. Disponível em: <https://tainacan.org/> Acesso em: 02 fev. de 2026. Temas para os repositórios digitais desenvolvidos com o plugin Tainacan.

THEMEFOREST. Disponível em: <https://themeforest.net/> Acesso em: 02 fev. de 2026.
Mercado com diversos temas premium para WordPress. Os produtos deste mercado em geral são mais confiáveis, mas é importante checar tema por tema antes de instalar, seguindo as instruções deste manual.

Temas oficiais do WordPress.org: Todo ano o WordPress.org lança um tema oficial, sendo que o último já vem junto com a instalação do WP. Todos eles são confiáveis.

Plugins WordPress

ADVANCED CUSTOM FIELDS. Disponível em: <https://www.advancedcustomfields.com/> Acesso em: 02 fev. de 2026. Plugin que permite acrescentar campos customizados no website.

AKISMET. Disponível em: <https://akismet.com/> Acesso em: 02 fev. de 2026.
Plugin para barrar spams em comentários.

ALLY ACESSIBILIDADE. Disponível em: <https://elementor.com/products/ally-web-accessibility/> Acesso em: 02 fev. de 2026. Plugin que acrescenta recursos de acessibilidade no website.

BBPRESS. Disponível em: <https://wordpress.org/plugins/bbpress/> Acesso em: 02 fev. de 2026. Plugin para acrescentar o recurso de fóruns no website.

BUDDYPRESS. Disponível em: <https://wordpress.org/plugins/buddypress/> Acesso em: 02 fev. de 2026. Plugin para acrescentar o recurso de intranet ou redes sociais no website.

CFBD7. Disponível em: <https://br.wordpress.org/plugins/contact-form-cfdb7/> Acesso em: 02 fev. de 2026. Plugin que registra em um banco de dados as submissões no formulário do Contact Form 7.

CLICKY ANALYTICS. Disponível em: <https://br.wordpress.org/plugins/clicky-analytics/> Acesso em: 02 fev. de 2026. Plugin da Clicky que permite geração de estatísticas de acesso ao website, seguindo as leis gerais de proteção de dados, como LGPD e GDPR.

CODECANYON. Disponível em: <https://codecanyon.net/> Acesso em: 02 fev. de 2026.
Mercado da Envato para plugins do WordPress, dentre outros. Os plugins deste mercado em geral são confiáveis, mas é importante checar um por um antes de instalar, seguindo as instruções deste manual.

CONTACTFORM7. Disponível em: <https://contactform7.com/> Acesso em: 02 fev. de 2026.
Plugin para formulários de contato e pesquisa avançados.

COOKIEYES. Disponível em: <https://br.wordpress.org/plugins/cookie-law-info/> Acesso em: 02 fev. de 2026. Plugin que acrescenta formulários de consentimento de cookies e outras demandas das leis gerais de proteção de dados, como a LGPD e GDPR.

FILEBIRD. Disponível em: <https://ninjateam.org/wordpress-media-library-folders/> Acesso em: 02 fev. de 2026. Plugin que permite organizar as mídias do WordPress em pastas.

JETPACK. Disponível em: <https://br.wordpress.org/plugins/jetpack/> Acesso em: 02 fev. de 2026.
Plugin com várias funções, incluindo cibersegurança e velocidade.

REDIRECTION. Disponível em: < https://br.wordpress.org/plugins/redirection/> Acesso em: 02 fev. de 2026. Plugin para redirecionamento de páginas.

SIMPLE CAPTCHA ALTERNATIVE WITH CLOUDFLARE TURNSTILE. Disponível em: <https://br.wordpress.org/plugins/simple-cloudflare-turnstile/> Acesso em: 02 fev. de 2026.
Plugin que permite acrescentar o Cloudflare Turnstile nos formulários (mensagem que verifica se o visitante não é um robô, em substituição ao CAPTCHA).

SLIDER REVOLUTION. Disponível em: <https://www.sliderrevolution.com/> Acesso em: 02 fev. de 2026. Plugin para desenvolver animações e designs avançados no website.

TAINACAN. Disponível em: <https://tainacan.org/> Acesso em: 02 fev. de 2026.
Plugin para desenvolvimento de repositórios digitais profissionais.

UPDRAFTPLUS. Disponível em: <https://updraftplus.com/> Acesso em: 02 fev. de 2026.
Plugin para backup do website e repositório digital.

UPSOLUTION CORE. Disponível em: <https://help.us-themes.com/impreza/us-core/> Acesso em: 02 fev. de 2026. Plugin para quem utiliza os temas Impreza ou Zephyr.

WORDFENCE. Disponível em: <https://www.wordfence.com/> Acesso em: 02 fev. de 2026. Plugins para segurança cibernética e controle de logins do website. Instalar o Wordfence Security e o Wordfence Login Security.

WP SUPER CACHE. Disponível em: < https://br.wordpress.org/plugins/wp-super-cache/> Acesso em: 02 fev. de 2026. Plugin que melhora a velocidade de acesso ao website.

WP BAKERY. Disponível em: <https://wpbakery.com/> Acesso em: 02 fev. de 2026. Plugin construtor de páginas avançadas e esteticamente mais elaboradas.

YOAST DUPLICATE POST. Disponível em: <https://br.wordpress.org/plugins/duplicate-post/> Acesso em: 02 fev. de 2026. Plugin que duplica posts e páginas.

YOAST SEO. Disponível em: <https://br.wordpress.org/plugins/wordpress-seo/> Acesso em: 02 fev. de 2026. Plugin que otimiza o website para mecanismos de busca e bots de IA.

Hospedagens

CLOUDFLARE. Disponível: <https://www.cloudflare.com/> Acesso em: 02 fev. de 2026. Plataforma com diversos recursos de CDN, segurança, estatísticas etc.

FAST COMET. Disponível em: <https://www.fastcomet.com/> Acesso em: 02 fev. de 2026. Empresa que atualmente hospeda os websites da autora deste manual.

HOSTINGER. Disponível em: <https://www.hostinger.com/br> Acesso em: 02 fev. de 2026. Empresa de hospedagem parceira do WordPress.org e já utilizada com sucesso pela autora deste manual.

WORDPRESS.COM Disponível em: <https://wordpress.com/> Acesso em: 02 fev. de 2026. Hospedagem de websites exclusivamente em WordPress, empresa de um dos criadores do WordPress e já utilizada com sucesso pela autora deste manual. Recomendada para usuários e GLAMs com poucos recursos, que desejam terceirizar todas as questões de hospedagem e instalação do WordPress para a empresa. Ou instituições GLAM e empresas de grande porte, que podem pagar mais pela comodidade e segurança que o WordPress.com oferece.

Softwares e Recursos Diversos

1PASSWORD. Disponível em: < https://1password.com/pt/> Acesso em: 02 fev. de 2026. Gerenciador e Gerador de Senhas.

BASECAMP. Disponível em: <https://basecamp.com/> Acesso em: 02 fev. de 2026. Software de gestão de projetos e rotinas.

BREVO. Disponível em: <https://www.brevo.com/pt/> Acesso em: 02 fev. de 2026. Plataforma de E-mail Marketing e CRM para Newsletters.

MCAFEE. Disponível em: <https://www.mcafee.com/pt-br/index.html> Acesso em: 02 fev. de 2026. Software antivírus e VPN.

MOODLE. Disponível em: <https://moodle.org/> Acesso em: 02 fev. de 2026. Sistema de Gestão de Ensino utilizado pela UFMG e inúmeras outras instituições.

MYSQL. Disponível em: <https://www.mysql.com/> Acesso em: 02 fev. de 2026. Banco de dados geralmente utilizado no WordPress.

PHPMYADMIN. Disponível em: <https://www.phpmyadmin.net/> Acesso em: 02 fev. de 2026. Software para administração dos bancos de dados MySQL.

PROTON. Disponível em: <https://proton.me/pt-br> Acesso em: 02 fev. de 2026. Plataforma de e-mail, VPN, calendário, drive de armazenamento, dentre outros recursos.

SIGNAL. Disponível em: <https://signal.org/pt_BR/> Acesso em: 02 fev. de 2026. Mensageiro melhor do que WhatsApp e Telegram em termos de cibersegurança e privacidade.

TODOIST. Disponível em: <https://todoist.com/> Acesso em: 02 fev. de 2026. Software de gestão de tarefas pessoal e para equipes.

WORDPRESS. Disponível em: <https://wordpress.org/> Acesso em: 02 fev. de 2026. Sistema de gestão de conteúdos mais utilizado no mundo para desenvolver websites.

VERA CRYPT. Disponível em: <https://www.veracrypt.fr/en/Downloads.html> Acesso em: 02 fev. de 2026. Criptografia de HDs e outros dispositivos eletrônicos.

Úteis

BUILT WITH. Disponível em: <https://builtwith.com/> Acesso em: 02 fev. de 2026.
Plataforma que fornece informações sobre o website a partir da URL – link de endereço, além de estatísticas úteis diversas sobre as tecnologias Web.

CERT. **Cartilhas e Glossário de Segurança na Internet.** Disponível em: <https://cartilha.cert.br/> Acesso em: 02 fev. de 2026.

DUCKDUCKGO. Disponível em: <https://duckduckgo.com/> Acesso em: 02 fev. de 2026.
Mecanismo de busca que respeita a sua privacidade, ao contrário do Google.

FIREFOX. Disponível em: <https://www.mozilla.org/en-US/firefox/> Acesso em: 02 fev. de 2026.
Navegador que respeita a sua privacidade.

INTERNET ARCHIVE. Disponível em: <https://archive.org/> Acesso em: 02 fev. de 2026.
Plataforma com inúmeros recursos, incluindo a possibilidade de criar o seu repositório digital de forma totalmente gratuita.

TOR. Disponível em: <https://www.torproject.org/> Acesso em: 02 fev. de 2026.
Navegador que aumenta o anonimato na navegação da Web e respeita sua privacidade.

Principais Referências deste Manual

AI SAFETY INSTITUTE – UK. Disponível em: <https://www.aisi.gov.uk/> Acesso em: 02 fev. de 2026.

BLANK, Grant; DUTTON, William. Perceived Threats to Privacy Online: The Internet in Britain. Oxford: Oxford Internet Institute, 2019.

CENTER FOR HUMANE TECHNOLOGY. Disponível em: <https://www.humanetech.com/> Acesso em: 02 fev. de 2026.

CERT. **Internet Segura**. Disponível em: <https://internetsegura.br/> Acesso em: 02 fev. de 2026.

CERT. **Vulnerability Notes Database.** Disponível em: <https://www.kb.cert.org/vuls/> Acesso em: 02 fev. de 2026.

CERT. **Materiais de Apoio para Grupos de Resposta a Incidentes de Segurança em Computadores (CSIRTs)**. Disponível em: <https://www.cert.br/csirts/> Acesso em: 02 fev. de 2026.

COLLECTIONS TRUST. Disponível em: <https://collectionstrust.org.uk/> Acesso em: 02 fev. de 2026.

CGI – COMITÊ GESTOR DA INTERNET NO BRASIL. Disponível em: <https://cgi.br/> Acesso em: 02 fev. de 2026.

CPNI. **Cyber Security**. Disponível em: <https://www.npsa.gov.uk/threat-and-risk-management> Acesso em: 02 fev. de 2026.

CVE. **Common Vulnerabilities and Exposures**. Disponível em: <https://www.cve.org/> Acesso em: 02 fev. de 2026.

GDPR EU. Disponível em: <https://gdpr.eu/> Acesso em: 02 fev. de 2026.

FUNCHAL, Rafael. **WordPress Security Checklist**. Disponível em: <https://wpsecuritychecklist.org/> Acesso em: 02 fev. de 2026.

HERZOG, Pete. **Open Source Security Testing Methodology Manual (OSSTMM)**. Disponível em: <https://www.isecom.org/> Acesso em: 02 fev. de 2026.

IASEAI. **Associação Internacional para a Inteligência Artificial Segura e Ética**. Disponível em: <https://www.iaseai.org/> Acesso em: 02 fev. de 2026.

LOPES, Brenner. **Curso de Segurança WordPress**. Disponível em: <https://cursos7.com.br/curso/curso-de-seguranca-wordpress/> Acesso em: 02 fev. de 2026.

LORD, Gail; LORD, Barry (org). **Manual of Digital Museum Planning**. EUA: Rowman & Littlefield Publishers, 2017.

MELLO, Janaina Cardoso de. Cibersegurança em gestão de museus no século 21 nas Humanidades Digitais. **Boletim do Tempo Presente**, Rio de Janeiro, vol. 10, n. 07. Jul. 2021. p. 12-28. Disponível em: <https://periodicos.ufs.br/tempopresente/article/view/16168> Acesso em: 02 fev. de 2026.

NATIONAL CYBERSECURITY ALLIANCE. Disponível em: <https://www.staysafeonline.org/pt/sobre-nos> Acesso em: 02 fev. de 2026.

NATIONAL CYBER SECURITY CENTRE UK. Disponível em: <https://www.ncsc.gov.uk/section/information-for/public-sector> Acesso em: 02 fev. de 2026.

NVD – NATIONAL VULNERABILITY DATABASE. Disponível em: <https://nvd.nist.gov/> Acesso em: 02 fev. de 2026.

PASSKEY CENTRAL. Disponível em: <https://www.passkeycentral.org/home/> Acesso em: 02 fev. de 2026.

PANAGIOTAKOPOULOS, Theodor. **GDPR in museums**. MOOC “Essential Digital Skills for Museum Professionals”, 2019.

SERPRO. **Fundamentos da Lei Geral de Proteção de Dados**. Disponível em: <https://www.escolavirtual.gov.br/> Acesso em: 02 fev. de 2026.

SUCURI. **An introduction to WordPress Security**. Disponível em: <https://sucuri.net/guides/wordpress-security/> Acesso em: 02 fev. de 2026.

TAINACAN. **Blindando o WordPress**. Disponível em: <https://tainacan.github.io/tainacan-wiki//#/optimization?id=blindando-o-wordpress> Acesso em: 02 fev. de 2026.

TODOROV, Todor; LUTFIU, Shpend. Cyber Risk Assessment Principles for Modern Digital Museums. **Digital Presentation and Preservation of Cultural and Scientific Heritage**, Sofia, Bulgária, v. 12, p. 235-242, 2022. ISSN 1314-4006.

WORDFENCE. **WordPress Security Fundamentals**. Disponível em: <https://www.wordfence.com/learn/> Acesso em: 02 fev. de 2026.

WORDFENCE BLOG. Disponível em: <https://www.wordfence.com/blog/> Acesso em: 02 fev. de 2026.

WORDPRESS. **Developer Resources**. Disponível em: <https://developer.wordpress.org/> Acesso em: 02 fev. de 2026.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância**. Rio de Janeiro: Intrínseca, 2021.

Divulgação Científica – Artigos e Livros para Leigos

ARMSTRONG, Ian. **Museums and galleries cannot afford to ignore cybersecurity if they want to consolidate the success of their digital pivot**. Disponível em: <https://www.museumnext.com/article/museums-and-galleries-cannot-afford-to-ignore-cybersecurity-if-they-want-to-consolidate-the-success-of-their-digital-pivot/>
Acesso em: 02 fev. de 2026.

BEAVER, Kevin. **Hacking para Leigos**. Rio de Janeiro: Alta Books, 2014.

CATHARINA DORIA – AI ETHICS EXPERT. Disponível em: <https://www.instagram.com/cahdoria/>
Acesso em: 03 mar. de 2026.

CUSEUM. **Cuseum's 8 Step Guide to Step Up Your Museum's Cybersecurity**. Disponível em: <https://cuseum.com/blog/2024/10/28/cuseums-8-step-guide-to-improve-your-museums-cybersecurity> Acesso em: 03 mar. de 2026.

Dark Web: Policiais se infiltram entre criminosos para salvar crianças – Documentário da BBC. Disponível em: <https://youtu.be/CYcAjdLN5TY?si=tuF2PC-LnCFW72fL> Acesso em: 03 mar. de 2026.

DREYFUSS, Emily. **Brazil's Museum Fire Proves Cultural Memory Needs a Digital Backup**. Disponível em: <https://www.wired.com/story/brazil-museum-fire-digital-archives/> Acesso em: 02 fev. de 2026.

IAMARINO, Átila. **Por que o iPhone é tão caro?** Disponível em: <https://www.youtube.com/watch?v=x9d6o8qpGpk> Acesso em: 02 fev. de 2026.

REYNOLDS, Matt. **Looking for alternatives to WhatsApp? Signal is your best bet**. Disponível em: <https://www.wired.co.uk/article/whatsapp-alternatives-vs-signal> Acesso em: 02 fev. de 2026.

STEINBERG, Joseph. **Cibersegurança para Leigos**. Rio de Janeiro: Alta Books, 2020.

TOLEDO. Luiz Fernando. **A brasileira que viraliza traduzindo o caos da IA**: "As pessoas estão perdidas". Disponível em: <https://www.bbc.com/portuguese/articles/c9v1292nrzro> Acesso em: 02 fev. de 2026.

UNITED STATES HOLOCAUST MEMORIAL MUSEUM. **Localizando as vítimas**. Disponível em: <https://encyclopedia.ushmm.org/content/pt-br/article/locating-the-victims> Acesso em: 02 fev. de 2026.

VEIGA, Ana Cecília Rocha. **Acervos Digitais e Museus: Gestão Inclusiva, Vício em Redes Sociais e Inteligência Artificial.** Disponível em: <https://anacecilia.digital/acervos-digitais-e-museus/> Acesso em: 02 fev. de 2026.

VEIGA, Ana Cecília Rocha. **Artigos sobre Cibersegurança e Privacidade de Dados**. Disponível em: <https://anacecilia.digital/tag/ciberseguranca/> Acesso em: 02 fev. de 2026.

VEIGA, Ana Cecília Rocha. **Como gerenciar uma comissão de avaliação de projetos ou seleção de candidatos no Basecamp?** Disponível em:<https://anacecilia.digital/gerenciar-comissao-no-basecamp/> Acesso em: 02 fev. de 2026.
Obs: No post são apresentadas as vantagens de se fazer a gestão de processos e tarefas em softwares adequados e não via e-mail e WhatsApp.

VEIGA, Ana Cecília Rocha. **Gestão do E-mail: Um guia completo para economizar tempo, reduzir o estresse e aumentar a produtividade.** Disponível em: <https://anacecilia.digital/gestao-do-e-mail-um-guia-completo-para-economizar-tempo-reduzir-o-estresse-e-aumentar-a-produtividade/> Acesso em: 02 fev. de 2026.
Obs: No post são apresentadas as vantagens do Proton, serviço suíço de e-mails que respeita a sua cibersegurança e privacidade de dados.

VEIGA, Ana Cecília Rocha. **O impacto da Inteligência Artificial nos Museus e no Setor Cultural.** Disponível em: <https://anacecilia.digital/o-impacto-da-inteligencia-artificial-nos-museus-e-no-setor-cultural/> Acesso em: 02 fev. de 2026.
Obs: Dentre estes impactos estão as questões de cibersegurança e privacidade de dados.

VEIGA, Ana Cecília Rocha. **Realidade Aumentada e Acessibilidade em Museus – MASP Labels**. Disponível em: <https://anacecilia.digital/realidade-aumentada-e-acessibilidade-em-museus/> Acesso em: 02 fev. de 2026.
Obs: Exemplo de hacktivismo ético envolvendo tecnologias digitais assistivas. Para ler outros casos de hacktivismo além do post, baixe o capítulo de livro disponível neste link.

VEIGA, Ana Cecília Rocha. **Tainacan – Vídeos e Tutoriais**. Disponível em: <https://anacecilia.digital/tag/tainacan/> Acesso em: 02 fev. de 2026.

VEIGA, Ana Cecília Rocha. **Vivendo sem WhatsApp e sem Telegram: como aumentar sua produtividade e qualidade de vida deletando estes apps**. Disponível em: <https://anacecilia.digital/vivendo-sem-whatsapp-e-sem-telegram-como-aumentar-sua-produtividade-e-qualidade-de-vida-deletando-estes-apps/> Acesso em: 02 fev. de 2026.
Obs: No post são apresentadas as vantagens do Signal, recomendado por sua segurança cibernética e privacidade de dados.

Agradecimentos do Projeto Recursos Web para GLAM

Pesquisa
PPGCI – Pós-Graduação em Ciência da Informação da UFMG (patrocínio para tradução da versão Beta do manual para o inglês, compartilhada com pesquisadores no exterior).
Diretoria da ECI/UFMG – Apoio institucional e acadêmico.
LTI da ECI/UFMG – Apoio técnico e de cibersegurança ao LavMUSEU e Tainacan Lab ECI UFMG, onde os testes desta pesquisa tomam curso.
Renato Nogueira Fontes – Tradução da Versão Beta para o Inglês.

Profissionais de Universidades e GLAMs
Araci Farhat de Carvalho – Técnico administrativo do Setor de Comunicação da Escola de Arquitetura da UFMG.
Alice Sá – Assistente de Comunicação do Espaço do Conhecimento UFMG.
Camila Mantovani – Coordenadora do Núcleo de Comunicação e Design do Espaço do Conhecimento UFMG.
Marcus Silveira – Técnico de Assuntos Educacionais da Rede de Museus da UFMG.

Sugestão de fontes e referências
Emmanuel Antunes Lima – Engenheiro Civil e pesquisador do LavMUSEU/UFMG.
Jeff Keese – Arquiteto, expógrafo e produtor cultural.
Marco Antônio Alves – Professor Adjunto da Faculdade de Direito da UFMG.
Rafael Funchal – Desenvolvedor Web, Funcionário da Automattic.
Roberto Ivo Fernandes Vaz – Ph.D. in Digital Media (Cum Laude) pela Universidade do Porto, NOVA Universidade de Lisboa e University of Texas at Austin - Portugal CoLab.

Revisão textual e argumentos
Alberto N. Veiga
Heloísa Rocha
Paulo Rocha

Anônimos
Agradecemos a todos os profissionais que colaboraram com o projeto, sendo que alguns preferiram permanecer anônimos.

Termos de Uso e Alerta de Responsabilidade

Ao elaborar este manual, procuramos consultar as melhores e mais atualizadas fontes disponíveis sobre Cibersegurança e Privacidade de Dados. Entretanto, não existe perfeição em nenhuma publicação, ainda mais sobre um assunto tão complexo, que se atualiza de um dia para o outro. E para o qual não há consenso sequer entre os próprios especialistas.

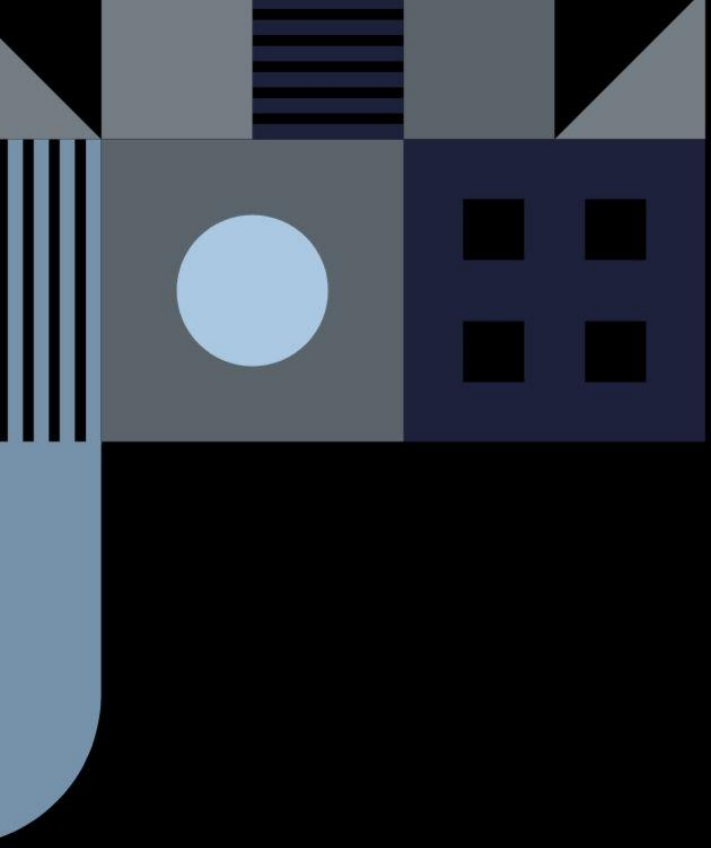
Portanto, como toda pesquisa de temas com este perfil, este manual possui suas limitações, desatualizações e possíveis falhas. Assim, ao usá-lo, você o aceita como está. E assume as responsabilidades por suas consequências, riscos, benefícios ou prejuízos.

Recomendamos, ainda, que sua instituição GLAM contrate funcionários especializados em cibersegurança ou consultores na implementação de políticas de privacidade e procedimentos de segurança física e cibernética.

Ou seja, este manual não substitui o trabalho de especialistas. Foi desenvolvido para que os profissionais de GLAM – galerias, bibliotecas, arquivos e museus – tenham conhecimentos mínimos e vocabulário técnico o suficiente para compreender a importância de se implementar protocolos de cibersegurança e privacidade de dados em suas instituições. Portanto, é um manual informativo e não formativo, tampouco esgota ou define este assunto.

Recomendamos, ainda, que confiram no website do projeto a existência de versões atualizadas e/ou corrigidas desta publicação: webmuseu.org/recursos

Caso tenha elogios, sugestões ou críticas a este manual, teremos imenso prazer em ouvi-las! Por gentileza, entre em contato com a autora.



ESCOLA de CIÊNCIA da INFORMAÇÃO
UFMG

75 ANOS
1950·2025

Projeto Recursos Web para GLAM

webmuseu.org/recursos