

2 de março de 2022

Resposta da Workiva ao ataque da Rússia à Ucrânia: Tempos voláteis exigem maior atenção

preparação para a segurança cibernética.

A Workiva segue à risca as diretrizes publicadas pela [iniciativaSHIELDS UPda U.S. Cybersecurity & Infrastructure Security Agency (CISO)e se comprometeu a compartilhar quaisquer incidentes ou atividades anômalas com as autoridades policiais competentes na(s) jurisdição(ões) onde a atividade ocorre.](https://www.cisa.gov/shields-up)

# Reduzir a probabilidade de uma intrusão cibernética prejudicial

**Valide que todos os acessos remotos à rede da organização e os acessos privilegiados ou administrativos**

**o acesso requer autenticação multifatorial.**

* A Workiva exige que todos os constituintes da Workiva usem o Single Sign On com Multi Factor Authentication. A Workiva recomenda que nossos clientes implementem o Single Sign On.

**Assegure-se de que o software esteja atualizado, priorizando as atualizações que tratam das**[**vulnerabilidadesexploradas conhecidas**](https://www.cisa.gov/known-exploited-vulnerabilities-catalog)  **e identificadas pela CISA.**

* A Workiva utiliza mecanismos automatizados de aplicação de patches para garantir que o software do host e do contêiner seja corrigido e atualizado. As vulnerabilidades identificadas em bibliotecas de terceiros incluídas em nosso aplicativo são priorizadas por gravidade e corrigidas como parte de nosso SDLC.

**Confirme se a equipe de TI da organização desativou todas as portas e protocolos que não são**

**essenciais para fins comerciais.**

* A Workiva estabeleceu e documentou nossas definições de configuração de acordo com as linhas de base do Center for Internet Security (CIS) e as listas de verificação compatíveis com o SCAP.

**Se a organização estiver usando serviços em nuvem, certifique-se de que o pessoal de TI tenha analisado e implementado** [**os fortes controles descritos na orientação da CISA.**](https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-013a)

* A Workiva obteve o FedRAMP Moderate e a ISO 27001:2013.
* Todo o acesso à Workiva é baseado em privilégios mínimos e requer o uso de IDs exclusivos com adesão às nossas políticas de senha, incluindo a exigência de logon único e autenticação de dois fatores. O acesso deve ser aprovado pelo gerente funcional e pelo sistema

proprietário, conforme gerenciado por meio de nosso sistema de tíquetes. Todas as atividades dentro da rede da Workiva e

são registrados em nossa ferramenta SIEM centralizada.

* A Workiva utiliza filtragem de spam de e-mail e bloqueia qualquer encaminhamento automático de e-mails. Além disso, os dispositivos e servidores executam ferramentas antimalware. Os funcionários passam por avaliações mensais de engenharia social.

**Inscreva-se nos** [**serviços gratuitos de higiene cibernética da CISA**](https://www.cisa.gov/cyber-hygiene-services)**, incluindo a verificação de vulnerabilidades, para ajudar a reduzir a exposição a ameaças**.

* Embora a Workiva não esteja qualificada para os serviços da CISA (não é um provedor de infraestrutura crítica), a Workiva é FedRAMP Moderate. Além disso, a Workiva fornece aos clientes relatórios de terceiros feitos por provedores autorizados pelo PCI/CREST para realizar varreduras e testes externos semestralmente, além de nossas varreduras e testes internos.

# Tome medidas para detectar rapidamente uma possível intrusão

**Certifique-se de que a equipe de segurança cibernética/TI esteja concentrada em identificar e avaliar rapidamente qualquer comportamento inesperado ou incomum da rede. Habilite o registro em log para investigar melhor os problemas ou eventos.**

* A Workiva utiliza nosso sistema de gerenciamento de eventos e informações de segurança (SIEM) para fornecer monitoramento contínuo e análise de registros. A equipe de segurança da informação da Workiva analisa os logs e alertas quanto a considerações de desempenho e segurança, incluindo logs relacionados a autenticação, endpoint, aplicativo da Web e muito mais. Os logs são armazenados em um sistema central de logs, transmitidos por um canal criptografado, criptografados em repouso e segregados de outros sistemas e usuários. Os registros não podem ser modificados depois de gravados e a exclusão do registro é monitorada. As informações de registro coletadas incluem informações como hora, tamanho dos dados, latência da resposta, tipo de transação, método de serviço da Web invocado, informações de usuário/conta/serviço, nome do host/ip, ação e/ou recursos envolvidos. Os registros são continuamente monitorados quanto a anormalidades e investigados de acordo com nossos padrões e políticas. Nossos alertas são continuamente revisados quanto à precisão, cobertura e eficácia, e os manuais são desenvolvidos e mantidos para padronizar e melhorar a resposta. Esses dados são usados para realizar investigações de eventos e incidentes de segurança relatados.
* Mais informações podem ser encontradas em nosso site de ajuda: [https://support.workiva.com/hc/en-](https://support.workiva.com/hc/en-us/articles/360035646392-View-Organization-Activities)  [us/articles/360035646392-View-Organization-Activities](https://support.workiva.com/hc/en-us/articles/360035646392-View-Organization-Activities)

**Confirme se toda a rede da organização está protegida por software antivírus/antimalware e se as assinaturas dessas ferramentas estão atualizadas.**

* Os dispositivos e servidores da Workiva são protegidos por software antimalware com proteção em tempo real e atualizações ativadas.

**Se estiver trabalhando com organizações ucranianas, tome cuidado extra para monitorar, inspecionar e isolar o tráfego dessas organizações; analise atentamente os controles de acesso a esse tráfego.**

* A Workiva não tem nenhuma operação na Ucrânia.

# Assegurar que a organização esteja preparada para reagir em caso de invasão.

**Designe uma equipe de resposta a crises com os principais pontos de contato para uma suspeita de incidente de segurança cibernética e funções/responsabilidades dentro da organização, incluindo tecnologia, comunicações, jurídico e continuidade dos negócios.**

* A equipe de Segurança da Informação da Workiva reconhece a necessidade de estar alerta aos riscos externos e está atenta à procura de possíveis problemas. Também empregamos o monitoramento ativo das principais informações usadas para identificar ameaças.

A Workiva mantém um plano de resposta a incidentes que aborda

* + Identificação
	+ Documentação
	+ Isolamento
	+ Resolução
	+ Comunicação
	+ Escalonamento

**Assegurar a disponibilidade do pessoal-chave; identificar meios de fornecer suporte de surto para responder a um incidente.**

* A Workiva mantém uma equipe de suporte 24 horas por dia, 7 dias por semana, com paginação de plantão para as equipes relevantes, que é testada anualmente como parte de nossos testes de continuidade de negócios e recuperação de desastres.

**Realize um exercício de mesa para garantir que todos os participantes entendam suas funções durante um incidente.**

* A Workiva realiza exercícios de mesa trimestrais, além de testes anuais de continuidade de negócios e recuperação de desastres para garantir que as equipes estejam bem familiarizadas com os planos da Workiva e conheçam suas respectivas funções.

# Maximizar a resistência da organização a um incidente cibernético destrutivo

**Teste os procedimentos de backup para garantir que os dados essenciais possam ser restaurados rapidamente se a organização for afetada por ransomware ou por um ataque cibernético destrutivo; certifique-se de que os backups estejam isolados das conexões de rede.**

* A Workiva utiliza backup de dados redundantes para oferecer recuperação pontual. Além disso, a Workiva permite que os clientes administrem suas contas por conta própria. A qualquer momento, um cliente pode salvar/exportar um documento ou excluir um documento. A Workiva apóia a economia

arquivos nos formatos DOCX (MS Word), XLSX (MS Excel) ou PDF (Adobe) para arquivamento em seus próprios sistemas.

* Ferramentas do cliente: [https://support.workiva.com/hc/en-us/articles/360035639692-Prepare-](https://support.workiva.com/hc/en-us/articles/360035639692-Prepare-for-the-Unexpected)  [for-the-Unexpected](https://support.workiva.com/hc/en-us/articles/360035639692-Prepare-for-the-Unexpected)

**Se estiver usando sistemas de controle industrial ou tecnologia operacional, realize um teste de controles manuais para garantir que as funções essenciais permaneçam operáveis se a rede da organização não estiver disponível ou não for confiável.**

* A Workiva não utiliza sistemas de controle industrial.
* Ao implementar as etapas acima, todas as organizações podem fazer progressos de curto prazo para melhorar a segurança cibernética e a resiliência. Além disso, embora os incidentes cibernéticos recentes não tenham sido atribuídos a agentes específicos, a CISA recomenda que o pessoal de segurança cibernética/TI de todas as organizações analise o documento [Understanding and Mitigating Russian State-Sponsored Cyber](https://www.cisa.gov/uscert/ncas/alerts/aa22-011a)  [Threats to U.S. Critical Infrastructure](https://www.cisa.gov/uscert/ncas/alerts/aa22-011a). A CISA também recomenda que as organizações visitem o [StopRansomware.gov](https://www.cisa.gov/stopransomware), uma página da Web centralizada e de todo o governo que fornece recursos e alertas sobre ransomware.
* Como agência de defesa cibernética do país, a CISA está disponível para ajudar as organizações a melhorar a segurança cibernética e a resiliência, inclusive por meio de especialistas em segurança cibernética designados em todo o país. No caso de um incidente cibernético, a CISA pode oferecer assistência às organizações vítimas e usar as informações dos relatórios de incidentes para proteger outras possíveis vítimas. Todas as organizações devem relatar incidentes e atividades anômalas à [CISA](https://www.cisa.gov/uscert/report) e/ou ao FBI por meio do [escritório local do FBI](https://www.fbi.gov/contact-us/field-offices) ou do CyWatch 24/7 do FBI pelo telefone (855) 292-3937 ou pelo siteCyWatch@fbi.gov.

# Recursos adicionais

* [**Insights da CISA: Preparing for and Mitigating Foreign Influence Operations Targeting**](https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf)[**Critical Infrastructure**](https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf) **(pdf) (fevereiro de 2022)**
* [**Insights da CISA: Implemente medidas de segurança cibernética agora para se proteger contra possíveis**](https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf)[**ameaças críticas**](https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf) **(pdf) (janeiro de 2022)**
* [**Alerta (AA22-011A) Entendendo e mitigando**](https://www.cisa.gov/uscert/ncas/alerts/aa22-011a)[**as ameaças**](https://www.cisa.gov/uscert/ncas/alerts/aa22-011a)**cibernéticas patrocinadas pelo Estado russo à infraestrutura crítica dos EUA (janeiro de 2022)**
* [**Insights da CISA: Preparando-se e mitigando possíveis ameaças cibernéticas**](https://www.cisa.gov/sites/default/files/publications/CISA_INSIGHTS-Preparing_For_and_Mitigating_Potential_Cyber_Threats-508C.pdf) **(pdf) (dezembro de 2021)**
* [**Lembrete para que a infraestrutura crítica permaneça vigilante contra ameaças durante feriados e**](https://www.cisa.gov/uscert/ncas/current-activity/2021/11/22/reminder-critical-infrastructure-stay-vigilant-against-threats)[**fins de semana**](https://www.cisa.gov/uscert/ncas/current-activity/2021/11/22/reminder-critical-infrastructure-stay-vigilant-against-threats) **(novembro de 2021)**
* [**Kit de ferramentas de desinformação sobre a COVID-19**](https://www.cisa.gov/publication/covid-19-disinformation-toolkit)
* [**Guia de planejamento e resposta a incidentes de desinformação, desinformação e malinformação (MDM) para**](https://www.cisa.gov/sites/default/files/publications/mdm-incident-response-guide_508.pdf)[**autoridades**](https://www.cisa.gov/sites/default/files/publications/mdm-incident-response-guide_508.pdf) **eleitorais**
* [**Guia de inicialização da página de controle de rumores do MDM**](https://www.cisa.gov/sites/default/files/publications/rumor-control-startup-guide_508.pdf)
* [**Visão geral e avisos sobre ameaças cibernéticas na Rússia**](https://www.cisa.gov/uscert/russia)
* [**Ferramentas e serviçosgratuitos de segurança cibernética para os setores públicoe privado**](https://www.cisa.gov/free-cybersecurity-tools-and-services)
* [**Guerra ao abacaxi**](https://www.cisa.gov/publication/war-pineapple)
* **Recursos externos**
* [**Kit de ferramentas de combate à desinformação RESIST 2 - GCS (civilservice.gov.uk)**](https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/)
* [**Agência Sueca de Contingências Civis (MSB) | Combate à desinformação**](https://counteringdisinformation.org/taxonomy/term/822)