**NISTIR 8374**

# Gestão de risco de ransomware:

*Um perfil do Framework de segurança cibernética*

William C. Barker
William Fisher
Karen Scarfone
Murugiah Souppaya

Esta publicação está disponível gratuitamente em:
https://doi.org/10.6028/NIST.IR.8374.por

National Institute of
Standards and Technology
U.S. Department of Commerce

**NISTIR 8374**

# Gestão de risco de ransomware:

*Um perfil do Framework de segurança cibernética*


William C. Barker
*Dakota Consulting*
*Silver Spring, MD*

Karen Scarfone
*Scarfone Cybersecurity*
*Clifton, VA*

William Fisher
*Divisão de Segurança Cibernética Aplicada*
*Laboratório de Tecnologia da Informação*

Murugiah Souppaya
*Divisão de Segurança Informática*
*Laboratório de Tecnologia da Informação*



Esta publicação está disponível gratuitamente em:
https://doi.org/10.6028/NIST.IR.8374.por

Fevereiro de 2022




Departamento de Comércio dos Estados Unidos
*Gina M. Raimondo, Secretária*

National Institute of Standards and Technology
*James K. Olthoff, diretor e subsecretário de comércio para padronização e tecnologia*
*do National Institute of Standards and Technology no desempenho de funções e responsabilidades não exclusivas*

Relatório interno ou interagências 8374 do National Institute of Standards and Technology
31 páginas (fevereiro de 2022)

Esta publicação está disponível gratuitamente em:
https://doi.org/10.6028/NIST.IR.8374.por



**Envie comentários sobre esta publicação para:** ransomware@nist.gov

National Institute of Standards and Technology
A/C: Divisão de Segurança Cibernética Aplicada, Laboratório de Tecnologia da Informação
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000



## Disclaimer

## Relatórios sobre Tecnologia de Sistemas Computacionais

O Laboratório de Tecnologia da Informação (ITL) do National Institute of Standards and Technology (NIST) tem o compromisso de fomentar a economia dos Estados Unidos e o bem-estar da população, fornecendo liderança técnica para a infraestrutura de medição e normas do país. O ITL desenvolve testes, métodos de teste, dados de referência, implementações de provas de conceito e análises técnicas para promover o desenvolvimento e uso produtivo da tecnologia da informação. As responsabilidades do ITL incluem o desenvolvimento de normas e diretrizes administrativas, técnicas, físicas e de gestão para a segurança e privacidade de informações, considerado o custo-benefício, em sistemas de informação federais, com exclusão daquelas relacionadas à segurança nacional.



## Resumo

Ransomware é um tipo de ataque malicioso em que os invasores criptografam os dados de uma organização e exigem pagamento para restaurar o acesso. Os invasores também podem roubar as informações de uma organização e exigir um pagamento adicional em troca de não divulgar as informações às autoridades, aos concorrentes ou ao público. Este Perfil de ransomware identifica os objetivos de segurança do Framework de segurança cibernética versão 1.1 que atendem à identificação, proteção, detecção, resposta e recuperação de eventos de ransomware. O perfil pode ser usado como um guia para gerenciar o risco de eventos de ransomware. Isso inclui ajudar a avaliar o nível de prontidão de uma organização para combater ameaças de ransomware e lidar com as possíveis consequências dos eventos.

## Palavras-chave

Framework de segurança cibernética; detecção; identificação; proteção; ransomware; recuperação; resposta; risco; segurança.

## Agradecimentos

Os autores agradecem a todos os indivíduos e organizações que contribuíram para a criação deste documento.

## Notificação de divulgação de patente

*NOTIFICAÇÃO: O ITL solicitou que os detentores de reivindicações de patentes cujo uso possa ser exigido para cumprir as orientações ou requisitos desta publicação divulguem tais reivindicações ao ITL. No entanto, os detentores de patentes não são obrigados a responder às solicitações do ITL. O ITL não pesquisou as patentes para identificar quais delas, se houver, podem ser aplicáveis a esta publicação.*

*Na data da publicação e na(s) solicitação(ões) seguinte(s) para identificação de reivindicações de patentes cujo uso possa ser necessário para o cumprimento das orientações ou requisitos desta publicação, nenhuma reivindicação de patente foi apresentada ao ITL.*

*O ITL não declara, de forma explícita ou implícita, que licenças não são necessárias para evitar violação de patente no uso desta publicação.*

## Índice

# 1 Introdução

Este Perfil de ransomware pode ajudar organizações e indivíduos a gerenciar o risco de eventos de ransomware. Isso inclui ajudar a avaliar o nível de prontidão de uma organização para combater ameaças de ransomware e lidar com as possíveis consequências dos eventos. O perfil também pode ser usado para identificar oportunidades de aprimoramento da segurança cibernética de forma a ajudar a impedir o ransomware. Ele mapeia os objetivos de segurança do Framework de aprimoramento da segurança cibernética para infraestrutura crítica, versão 1.1 [1] (também conhecido como Framework de segurança cibernética do NIST) em relação a recursos e medidas de segurança que ajudam na identificação, proteção, detecção, resposta e recuperação em caso de eventos de ransomware.

## 1.1 O desafio do ransomware

Ransomware é um tipo de malware que criptografa os dados de uma organização e exige pagamento como condição para restaurar o acesso a esses dados. O ransomware também pode ser usado para roubar informações de uma organização e exigir pagamento adicional em troca de não divulgar as informações às autoridades, concorrentes ou ao público. Os ataques de ransomware visam os dados ou a infraestrutura crítica da organização, interrompendo ou impedindo as operações e colocando um dilema para a gestão: pagar o resgate e esperar que os invasores mantenham sua palavra sobre restaurar o acesso e não divulgar os dados, ou não pagar o resgate e tentar restaurar as operações. Os métodos que o ransomware usa para obter acesso às informações e sistemas de uma organização são parecidos aos ataques cibernéticos de forma mais ampla, mas visam forçar o pagamento de um resgate. As técnicas usadas para divulgar o ransomware continuarão mudando, dado que os invasores estão constantemente procurando novas maneiras de pressionar suas vítimas.

Os ataques de ransomware diferem dos outros eventos de segurança cibernética que obtém acesso de forma clandestina a informações como propriedade intelectual, dados de cartão de crédito ou informações de identificação pessoal para posterior exfiltração e monetização. Em vez disso, o ransomware ameaça causar um impacto imediato nas operações comerciais. Durante um evento de ransomware, as organizações podem ter pouco tempo para mitigar ou remediar o impacto, restaurar sistemas ou se comunicar por meio dos canais de negócios, parceiros e relações públicas necessários. Por isso, é especialmente importante que as organizações estejam preparadas. Isso inclui instruir os usuários de sistemas cibernéticos, equipes de resposta e tomadores de decisões de negócios sobre a importância de saber prevenir e lidar com possíveis comprometimentos antes que eles ocorram, além dos processos e procedimentos envolvidos.

Felizmente, as organizações podem seguir as etapas recomendadas para se preparar e reduzir o risco de que os ataques de ransomware sejam bem-sucedidos. Isso inclui o seguinte: *identificar* e *proteger* dados, sistemas e dispositivos críticos; *detectar* eventos de ransomware o mais cedo possível (de preferência antes que o ransomware seja implantado); e preparar-se para *responder* e *recuperar-se* de quaisquer eventos de ransomware. Há muitos recursos disponíveis para ajudar as organizações nesses esforços. Eles incluem informações do NIST (National Institute of Standards and Technology), do FBI (Departamento Federal de Investigação) e do DHS (Departamento de Segurança Interna dos EUA). Encontre recursos adicionais do NIST no

Apêndice A deste documento.

Os recursos e medidas de segurança na Tabela 1 deste perfil atendem a uma abordagem detalhada para prevenir e mitigar eventos de ransomware. Percebendo que realizar todas essas medidas pode estar além do alcance de algumas pessoas, a caixa de texto abaixo inclui etapas preventivas básicas que uma organização pode tomar agora para se proteger contra a ameaça de ransomware. Nem todas essas medidas se aplicam às situações de todas as organizações. A orientação neste relatório aborda as melhores práticas, e não um conjunto de requisitos legais ou regulamentares.



**DICAS BÁSICAS DE RANSOMWARE**

*Mesmo sem realizar todas as medidas descritas neste Perfil de ransomware, existem algumas etapas preventivas básicas que uma organização pode tomar agora para se proteger e se recuperar da ameaça de ransomware. Elas incluem:*

1. **Instruir os funcionários sobre como evitar infecções por ransomware.**
   - **Não abrir arquivos ou clicar em links de fontes desconhecidas**, a menos que você primeiro execute uma verificação antivírus ou examine os links com cuidado.
   - **Evitar sites e aplicativos pessoais,** como e-mail, chat e mídias sociais, nos computadores de trabalho.
   - **Não conectar dispositivos pessoais a redes de trabalho sem autorização prévia**.
2. **Evitar vulnerabilidades em sistemas que o ransomware possa explorar.**
   - **Manter os sistemas relevantes totalmente corrigidos.** Executar verificações programadas para identificar correções disponíveis e instalar todas elas assim que possível.
   - **Aplicar princípios de zero trust em todos os sistemas em rede.** Gerenciar o acesso a todas as funções de rede e segmentar redes internas sempre que possível para evitar que o malware se prolifere entre sistemas que podem ser afetados.
   - **Permitir a instalação e execução apenas de aplicativos autorizados.** Configurar sistemas operacionais e/ou software de terceiros para executar apenas aplicativos autorizados. Isso também pode ser feito adotando-se uma política de revisão e para então adicionar ou remover aplicativos autorizados em uma lista de permissões.
   - **Informar seus fornecedores de tecnologia sobre suas expectativas** (por exemplo, em linguagem contratual) de que eles aplicarão medidas para desencorajar ataques de ransomware.
3. **Detectar e interromper rapidamente ataques e infecções de ransomware.**
   - **Usar sempre software de detecção de malware, como software antivírus.** Configurá-lo para verificar automaticamente e-mails e pen drives.
   - **Monitorar continuamente** os serviços de diretório (e outros repositórios de usuários primários) em busca de indicadores de comprometimento ou ataque ativo.

- **Bloquear o acesso a recursos da Web não confiáveis.** Usar produtos ou serviços que bloqueiem o acesso a nomes de servidores, endereços IP ou portas e protocolos conhecidos por serem maliciosos ou suspeitos de serem indicadores de atividade maliciosa do sistema. Isso inclui o uso de produtos e serviços que fornecem proteção de integridade para o componente de domínio de endereços (por exemplo, hacker@poser.com).

4. **Dificultar a propagação do ransomware.**
   - **Usar contas de usuário padrão** com autenticação multifator versus contas com privilégios administrativos sempre que possível.
   - **Introduzir atrasos de autenticação ou configurar o bloqueio automático de contas** como uma defesa contra tentativas automatizadas de adivinhar senhas.
   - **Atribuir e gerenciar a autorização de credenciais** para todos os ativos e softwares da empresa e verificar periodicamente se cada conta tem apenas o acesso necessário seguindo o princípio do menor privilégio.
   - **Armazenar os dados em um formato imutável** (para que o banco de dados não sobrescreva automaticamente os dados mais antigos quando novos dados forem disponibilizados).
   - **Permitir o acesso externo a recursos de rede internos somente por meio de conexões VPN (rede virtual privada) seguras.**
5. **Facilitar a recuperação de informações armazenadas de um futuro evento de ransomware.**
   - **Fazer um plano de recuperação de incidentes.** Desenvolver, implementar e exercer regularmente um plano de recuperação de incidentes com funções e estratégias definidas para a tomada de decisões. Isso pode ser parte de um plano de continuidade de operações. O plano deve identificar serviços de missão crítica e outros serviços essenciais para permitir a priorização de recuperação e planos de continuidade de negócios para esses serviços críticos.
   - **Fazer backup de dados, proteger backups e testar a restauração.** Planejar, implementar e testar cuidadosamente uma estratégia de backup e restauração de dados e proteger e isolar backups de dados importantes.
   - **Manter seus contatos.** Manter uma lista atualizada de contatos internos e externos para ataques de ransomware, incluindo aplicação da lei, assessoria jurídica e recursos de resposta a incidentes.



## 1.2 Público-alvo

O Perfil de ransomware é destinado a qualquer organização com recursos cibernéticos que possam estar sujeitos a ataques de ransomware, independentemente do setor ou tamanho. Qualquer organização, incluindo pequenas e médias empresas (SMBs), pequenas agências federais e outras pequenas organizações e operadores de sistemas de controle industrial (ICS) ou tecnologias operacionais (OT), pode aproveitar essa orientação e é incentivada também a analisar

o Framework de segurança cibernética.

Muitas dessas ações podem ser realizadas sem gastar recursos consideráveis. Valor especial pode ser obtido por organizações que:

- estão familiarizadas com o Framework de segurança cibernética do NIST – talvez já o tenham adotado – para ajudar a identificar, avaliar e gerenciar riscos de segurança cibernética e desejam aprimorar suas posturas de risco abordando preocupações de ransomware;
- não estão familiarizadas com o Framework de segurança cibernética, mas desejam implementar frameworks de gestão de risco para enfrentar ameaças de ransomware.

### 1.3 Recursos de orientação adicionais

Além dos recursos citados anteriormente nesta seção, o National Cybersecurity Center of Excellence (NCCoE) do NIST produziu orientações para atender à mitigação de ameaças de ransomware. O NIST tem muitos outros recursos que, embora não sejam específicos de ransomware, contêm informações importantes sobre identificação, proteção, detecção, resposta e recuperação de eventos de ransomware. Consulte a seção Referências para obter uma lista de referências e o Apêndice A deste perfil com uma lista mais extensa de recursos do NIST.

## 2 O Perfil de ransomware

O Perfil de ransomware alinha os requisitos, objetivos, apetite de risco e recursos de prevenção e mitigação de ransomware das organizações com os elementos do Framework de segurança cibernética do NIST. Ele deve ajudar as organizações a identificar e priorizar oportunidades para aprimorar sua segurança e resiliência contra ataques de ransomware. As organizações podem usar este documento como um guia para traçar o perfil do estado de sua própria prontidão. Isso ajudará a determinar seu "perfil" ou estado atual e definir um "perfil ideal" para identificar lacunas.

A Tabela 1 define o Perfil de ransomware. As duas primeiras colunas listam Categorias e Subcategorias relevantes do Framework de segurança cibernética que as organizações podem usar como resultados ideias para seus programas de gestão de risco de ransomware. A terceira coluna explica brevemente como cada Subcategoria ajuda na identificação, proteção, detecção, resposta e recuperação em caso de eventos de ransomware.

Este perfil também cita "Referências informativas". Essas seções especificam padrões, diretrizes e práticas comuns entre os setores de infraestrutura crítica que ilustram um método para alcançar os resultados associados a cada subcategoria. As Referências informativas no Framework de segurança cibernética são ilustrativas e não exaustivas. Elas são baseadas em orientações intersetoriais mais frequentemente consultadas durante o processo de desenvolvimento do Framework.

Por exemplo, a segunda coluna da Tabela 1 cita requisitos relevantes de duas das referências informativas incluídas no Framework de segurança cibernética do NIST: Organização Internacional para Padronização/Comissão Eletrotécnica Internacional (ISO/IEC) 27001:2013, *Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos* [2] e NIST SP 800-53 Revisão 5, *Controles de segurança e privacidade para sistemas de informação e organizações* [3].

O Framework de segurança cibernética lista Referências informativas adicionais para cada Subcategoria. Essas referências serão atualizadas periodicamente nas versões online deste documento de orientação.

Veja a seguir as cinco funções do Framework de segurança cibernética usadas para organizar as categorias:

- **Identificação** – Desenvolver uma compreensão organizacional para gerenciar os riscos de segurança cibernética referente a sistemas, pessoas, ativos, dados e recursos. As atividades na função Identificação são fundamentais para o uso eficaz do Framework. Compreender o contexto de negócios, os recursos que atendem a funções críticas e os riscos de segurança cibernética relacionados permite que uma organização foque e priorize seus esforços, de forma consistente com sua estratégia de gestão de riscos e necessidades de negócios.

- **Proteção** – Desenvolver e implementar as medidas de segurança adequadas para garantir a entrega dos serviços essenciais. A função Proteção atende à capacidade de limitar ou conter o impacto de um possível evento de segurança cibernética.
- **Detecção** – Desenvolver e implementar as atividades adequadas para identificar a ocorrência de um evento de segurança cibernética. A função Detecção permite a descoberta oportuna de eventos de segurança cibernética.
- **Resposta** – Desenvolver e implementar as atividades adequadas para agir durante a detecção de um incidente de segurança cibernética. A função Resposta atende à capacidade de conter o impacto de um possível incidente de segurança cibernética.
- **Recuperação** – Desenvolver e implementar as atividades adequadas para manter os planos de resiliência e restaurar quaisquer recursos ou serviços afetados devido a um incidente de segurança cibernética. A função Recuperação atende à recuperação oportuna das operações normais para reduzir o impacto de um incidente de segurança cibernética.

**Tabela 1: Perfil de gestão de risco de ransomware**

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| **Identificação** | | |
| **Gestão de ativos (ID.AM):** Os dados, pessoal, dispositivos, sistemas e instalações que permitem que a organização atinja os objetivos de negócios são identificados e gerenciados de acordo com sua importância relativa para os objetivos organizacionais e a estratégia de risco da organização. | **ID.AM-1:** Dispositivos físicos e sistemas dentro da organização são inventariados<br>**ISO/IEC 27001:2013** A.8.1.1, A.8.1.2<br>**NIST SP 800-53 Rev. 5** CM-8, PM-5 | Um inventário de dispositivos físicos deve ser realizado, revisado e mantido para garantir que esses dispositivos não sejam vulneráveis a ransomware. Também seria recomendável ter um inventário de hardware durante as fases de recuperação após um ataque de ransomware, caso seja necessário reinstalar aplicativos. |
| | **ID.AM-2:** Plataformas de software e aplicativos dentro da organização são inventariados<br>**ISO/IEC 27001:2013** A.8.1.1, A.8.1.2<br>**NIST SP 800-53 Rev. 5** CM-8, PM-5 | Os inventários de software podem rastrear informações como nome e versão do software, dispositivos onde está instalado atualmente, data da última correção e vulnerabilidades atuais conhecidas. Essas informações atendem à correção de vulnerabilidades que podem ser exploradas em ataques de ransomware. |
| | **ID.AM-3:** A comunicação organizacional e os fluxos de dados são mapeados<br>**ISO/IEC 27001:2013** A.13.2.1, A.13.2.2<br>**NIST SP 800-53 Rev. 5** AC-4, CA-3, CA-9, PL-8 | Isso ajuda a enumerar quais informações ou processos estão em risco, caso os invasores se movam lateralmente em um ambiente. |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| | **ID.AM-4:** Os sistemas de informação externos são catalogados<br>**ISO/IEC 27001:2013** A.11.2.6<br>**NIST SP 800-53 Rev. 5** AC-20, SA-9 | Isso é importante para planejar comunicações com parceiros e possíveis ações para se desconectar temporariamente de sistemas externos em resposta a eventos de ransomware. A identificação dessas conexões também ajudará as organizações a planejar a implementação do controle de segurança e a identificar áreas onde os controles podem ser compartilhados com terceiros. |
| | **ID.AM-5:** Os recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base em sua classificação, criticidade e valor comercial<br>**ISO/IEC 27001:2013** A.8.2.1<br>**NIST SP 800-53 Rev. 5** CP-2, RA-2, RA-9, SC-6 | Isso é essencial para entender o verdadeiro escopo e impacto dos eventos de ransomware e é importante no planejamento de contingência para futuros eventos de ransomware, resposta a emergências e ações de recuperação. Ajuda as equipes de operações e incidentes a priorizar recursos e atende ao planejamento de contingência para futuros eventos de ransomware, resposta a emergências e ações de recuperação. Se houver um sistema de controle industrial (ICS) associado, suas funções críticas deverão ser incluídas nas ações de resposta e recuperação de emergência. |
| | **ID.AM-6:** As funções e responsabilidades de segurança cibernética para toda a força de trabalho e partes interessadas de terceiros (por exemplo, fornecedores, clientes, parceiros) são estabelecidas<br>**ISO/IEC 27001:2013** A.6.1.1<br>**NIST SP 800-53 Rev. 5** CP-2, PM-11, PS-7 | É importante que todos na organização entendam suas funções e responsabilidades para prevenir eventos de ransomware e, se aplicável, responder e recuperar de eventos de ransomware. Essas funções e responsabilidades devem ser formalmente documentadas em um plano de resposta a incidentes. O plano de resposta a incidentes deve especificar o exercício regular do plano (por exemplo, executar simulações de resposta a incidentes pelo menos anualmente). |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| **Ambiente empresarial (ID.BE):** A missão, os objetivos, as partes interessadas e as atividades da organização são compreendidas e priorizadas; essas informações são usadas para informar funções, responsabilidades e decisões de gestão de risco de segurança cibernética. | **ID.BE-2:** O lugar da organização na infraestrutura crítica e seu setor industrial são identificados e comunicado<br>**ISO/IEC 27001:2013** Cláusula 4.1<br>**NIST SP 800-53 Rev. 5** PM-8 | Isso permite que as equipes nacionais de resposta a incidentes de segurança informática entendam melhor o lugar da organização visada no ambiente de infraestrutura crítica e permite que elas reajam a tempo no caso de impactos intersetoriais. Isso também incentiva a organização e suas partes interessadas externas a considerar os efeitos a jusante do ataque de ransomware. |
| | **ID.BE-3:** As prioridades para a missão, objetivos e atividades organizacionais são estabelecidas e comunicadas<br>**NIST SP 800-53 Rev. 5** PM-11, SA-14 | Isso ajuda as equipes de operações e incidentes a priorizar recursos. Atende ao planejamento de contingência para futuros eventos de ransomware, resposta a emergências e ações de recuperação. |
| | **ID.BE-4:** Dependências e funções críticas para entrega de serviços críticos são estabelecidas<br>**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3<br>**NIST SP 800-53 Rev. 5** CP-8, PE-9, PE-11, PM-8, SA-20 | Isso ajuda a identificar componentes secundários e terciários críticos no atendimento às principais funções de negócios da organização. Isso é necessário para priorizar planos de contingência para eventos futuros e respostas de emergência a eventos de ransomware. Se houver um ICS associado, suas funções críticas deverão ser incluídas nas ações de resposta e recuperação de emergência. |
| **Governança (ID.GV):** As políticas, procedimentos e processos para gerenciar e monitorar os requisitos regulamentares, legais, de risco, ambientais e operacionais da organização são entendidos e informam a gestão de risco de segurança cibernética. | **ID.GV-1:** A política de segurança cibernética organizacional é estabelecida e comunicada<br>**ISO/IEC 27001:2013** A.5.1.1<br>**NIST SP 800-53 Rev. 5** AC-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, PE-01, PL-01, PM-01, RA-01, SA-01, SC-01, SI-01 | Estabelecer e comunicar as políticas necessárias para prevenir ou mitigar eventos de ransomware é essencial e fundamental para todas as outras atividades de prevenção e mitigação. Sempre que for possível, essas políticas devem ser revisadas periodicamente para refletir a natureza dinâmica do risco e a realidade dos ajustes contínuos necessários. |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| | **ID.GV-3:** Os requisitos legais e regulamentares relacionados à segurança cibernética, incluindo obrigações de privacidade e liberdades civis, são entendidos e gerenciados<br><br>**ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5<br><br>**NIST SP 800-53 Rev. 5** CA-07, RA-02 | Isso é necessário para desenvolver políticas de segurança cibernética e estabelecer prioridades no planejamento de contingência para resposta a futuros eventos de ransomware. |
| | **ID.GV-4:** Os processos de governança e gestão de risco abordam os riscos de segurança cibernética<br><br>**ISO/IEC 27001:2013** Cláusula 6<br><br>**NIST SP 800-53 Rev. 5** PM-3, PM-7, PM-9, PM-10, PM-11, SA-2 | Os riscos de ransomware devem ser considerados na governança de gestão de risco organizacional para estabelecer políticas de segurança cibernética adequadas. |
| **Avaliação de risco (ID.RA):** A organização entende o risco de segurança cibernética para as operações organizacionais (incluindo missão, funções, imagem ou reputação), ativos organizacionais e indivíduos. | **ID.RA-1:** As vulnerabilidades dos ativos são identificadas e documentadas<br><br>**ISO/IEC 27001:2013** A.12.6.1, A.18.2.3<br><br>**NIST SP 800-53 Rev. 5** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 | Identificar e documentar as vulnerabilidades dos ativos da organização é crucial para desenvolver planos e priorizar a mitigação ou eliminação dessas vulnerabilidades. Essas ações também são essenciais para o planejamento de contingência para avaliar e responder a futuros eventos de ransomware e reduzirão a probabilidade de um ataque de ransomware bem-sucedido. |
| | **ID.RA-2:** A inteligência de ameaças cibernéticas é recebida de fóruns e fontes de compartilhamento de informações<br><br>**ISO/IEC 27001:2013** A.6.1.4<br><br>**NIST SP 800-53 Rev. 5** PM-15, PM-16, SI-5 | Receber e usar inteligência de ameaças cibernéticas de fontes de compartilhamento de informações pode reduzir a exposição a ataques de ransomware e facilitar a detecção precoce de novas ameaças. |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| | **ID.RA-4:** Os potenciais impactos e probabilidades de negócios são identificados<br>**ISO/IEC 27001:2013** A.16.1.6, Cláusula 6.1.2<br>**NIST SP 800-53 Rev. 5** PM-9, PM-11, RA-2, RA-3, SA-20 | Compreender os impactos nos negócios de possíveis eventos de ransomware é necessário para atender a análises de custo-benefício de segurança cibernética, bem como para estabelecer prioridades das atividades em planos de resposta e recuperação de ransomware. Compreender os possíveis impactos nos negócios também atende às decisões de resposta de emergência no caso de um ataque de ransomware. |
| | **ID.RA-6:** As respostas aos riscos são identificadas e priorizadas<br>**ISO/IEC 27001:2013** Cláusula 6.1.3<br>**NIST SP 800-53 Rev. 5** PM-4, PM-9 | A despesa associada à resposta e recuperação de eventos de ransomware é diretamente afetada pela eficácia do planejamento de contingência para respostas a riscos projetados. |
| **Estratégia de gestão de riscos (ID.RM):** As prioridades, restrições, tolerâncias de risco e premissas da organização são estabelecidas e usadas para atender às decisões de risco operacional. | **ID.RM-1:** Os processos de gestão de riscos são estabelecidos, gerenciados e acordados pelas partes interessadas organizacionais<br>**ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3, Cláusula 9.3<br>**NIST SP 800-53 Rev. 5** PM-4, PM-9 | Estabelecer e fazer cumprir as políticas, funções e responsabilidades organizacionais depende de as partes interessadas concordarem e implementarem processos eficazes de gestão de riscos. Os processos devem levar em consideração o risco de um evento de ransomware. Essas políticas devem ser revisadas periodicamente para refletir a natureza dinâmica do risco e a realidade dos ajustes necessários ao longo do tempo. |
| **Gestão de riscos da cadeia de suprimentos (ID.SC):** As prioridades, restrições, tolerâncias de risco e premissas da organização são estabelecidas e usadas para atender às decisões de risco associadas à gestão do risco da cadeia de suprimentos. A organização estabeleceu e implementou os processos para identificar, avaliar e gerenciar os riscos da cadeia de suprimentos. | **ID.SC-5:** O planejamento e os testes de resposta e recuperação são realizados com fornecedores e provedores terceirizados<br>**ISO/IEC 27001:2013** A.17.1.3<br>**NIST SP 800-53 Rev. 5** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9 | O planejamento de contingência de ransomware deve ser coordenado com fornecedores e terceiros e deve incluir testes de atividades planejadas. O plano deve incluir um cenário em que a organização, seus fornecedores e provedores terceirizados sejam afetados pelo ransomware. |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| **Proteção** | | |
| **Gestão de identidade, autenticação e controle de acesso (PR.AC):** O acesso a ativos físicos e lógicos e a instalações associadas é limitado a usuários, processos e dispositivos autorizados, além de ser gerenciado de acordo com o risco avaliado de acesso não autorizado a atividades e transações autorizadas. | **PR.AC-1:** Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados<br>**ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3<br>**NIST SP 800-53 Rev. 5** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 | A maioria dos ataques de ransomware é realizada por meio de conexões de rede, e os ataques de ransomware geralmente começam com o comprometimento de credenciais (por exemplo, compartilhamento não autorizado ou captura de identidade de login e senha). A gestão adequada de credenciais é essencial, embora não seja a única mitigação necessária. |
| | **PR.AC-3:** O acesso remoto é gerenciado<br>**ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1<br>**NIST SP 800-53 Rev. 5** AC-1, AC-17, AC-19, AC-20, SC-15 | A maioria dos ataques de ransomware é realizada remotamente. A gestão de privilégios associados ao acesso remoto pode ajudar a manter a integridade de sistemas e arquivos de dados para proteção contra inserção de código malicioso e exfiltração de dados. Usar a autenticação multifator é uma maneira importante e de fácil implementação para reduzir a probabilidade de comprometimento da conta. |
| | **PR.AC-4:** As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de funções<br>**ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5<br>**NIST SP 800-53 Rev. 5** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 | Muitos eventos de ransomware ocorrem comprometendo as credenciais do usuário ou invocando processos que têm acesso privilegiado desnecessário aos sistemas. Esse é um passo muito importante na gestão para prevenir esses eventos. |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| | **PR.AC-5:** A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)<br>**ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3<br>**NIST SP 800-53 Rev. 5** AC-4, AC-10, SC-7 | A segmentação ou segregação de rede pode limitar o escopo dos eventos de ransomware impedindo que o malware se prolifere entre sistemas que podem ser afetados (por exemplo, ter acesso a uma tecnologia operacional ou sistema de controle partindo de uma rede de tecnologia da informação comercial). É fundamental separar as redes de TI e OT e validar regularmente sua independência. Isso não apenas reduz o risco de comprometimento dos sistemas OT, mas também permite que as operações críticas de nível inferior continuem enquanto os sistemas de TI de negócios se recuperam do ransomware. Isso é particularmente importante para funções críticas de ICS, incluindo Sistemas de instrumentos de segurança (SIS). |
| | **PR.AC-6:** As identidades são comprovadas e vinculadas a credenciais e confirmadas em interações<br>**ISO/IEC 27001:2013** A.7.1.1, A.9.2.1<br>**NIST SP 800-53 Rev. 5** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3 | Credenciais comprometidas são um vetor de ataque comum em eventos de ransomware. As identidades devem ser comprovadas e, em seguida, vinculadas a uma credencial (por exemplo, autenticação de dois fatores de indivíduos formalmente autorizados) para limitar a probabilidade de que as credenciais sejam comprometidas ou emitidas para um indivíduo não autorizado. |
| **Conscientização e treinamento (PR.AT):** O pessoal e os parceiros da organização recebem orientações de conscientização sobre segurança cibernética e são treinados para desempenhar suas funções e responsabilidades relacionadas à segurança cibernética de acordo com as políticas, procedimentos e acordos relacionados. | **PR.AT-1:** Todos os usuários são informados e treinados<br>**ISO/IEC 27001:2013** A.7.2.2, A.12.2.1<br>**NIST SP 800-53 Rev. 5** AT-2, PM-13 | A maioria dos ataques de ransomware é possibilitada por usuários que se envolvem em práticas inseguras, administradores que implementam configurações inseguras ou desenvolvedores com treinamento de segurança insuficiente. |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| **Segurança de dados (PR.DS):** Informações e registros (dados) são gerenciados de forma consistente com a estratégia de risco da organização para proteger a confidencialidade, integridade e disponibilidade das informações. | **PR.DS-4:** Capacidade adequada para garantir que a disponibilidade seja mantida<br>**ISO/IEC 27001:2013** A.12.1.3, A.17.2.1<br>**NIST SP 800-53 Rev. 5** AU-4, CP-2, SC-5 | Garantir a disponibilidade adequada de dados pode reduzir os impactos do ransomware. Isso inclui a capacidade de manter backups de dados fora do local e offline, testando o tempo médio de recuperação e a redundância do sistema, quando necessário. |
| | **PR.DS-5:** Proteções contra vazamentos de dados são implementadas<br>**ISO/IEC 27001:2013** A.12.1.3, A.17.2.1<br>**NIST SP 800-53 Rev. 5** AU-4, CP-2, SC-5 | A extorsão dupla, ou seja, exigência de pagamento para restaurar o acesso aos dados *e* para não vender ou publicar os dados em outro lugar, é comum. Por isso, as soluções de prevenção de vazamento de dados são importantes. |
| | **PR.DS-6:** Mecanismos de verificação de integridade são usados para verificar a integridade do software, firmware e informações<br>**ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4<br>**NIST SP 800-53 Rev. 5** SC-16, SI-7 | Mecanismos de verificação de integridade podem detectar atualizações de software adulteradas que podem ser usadas para inserir malware que permite eventos de ransomware. |
| | **PR.DS-7:** O(s) ambiente(s) de desenvolvimento e teste são separados do ambiente de produção<br>**ISO/IEC 27001:2013** A.12.1.4<br>**NIST SP 800-53 Rev. 5** CM-2 | Manter os ambientes de desenvolvimento e teste separados dos ambientes de produção pode impedir que o ransomware seja propagado dos sistemas de desenvolvimento e teste para os sistemas de produção. |
| **Processos e procedimentos de proteção da informação (PR.IP):** Políticas de segurança (que abordam propósito, escopo, funções, responsabilidades, compromisso de gestão e coordenação entre entidades organizacionais), processos e procedimentos são mantidos e usados para gerenciar a proteção de sistemas e ativos de informação. | **PR.IP-1:** Uma configuração básica de sistemas de tecnologia da informação/controle industrial é criada e mantida incorporando princípios de segurança (por exemplo, conceito de funcionalidade mínima)<br>**ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4<br>**NIST SP 800-53 Rev. 5** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 | As linhas de base são úteis para estabelecer o conjunto de funções que um sistema precisa executar para que qualquer desvio dessa linha de base possa ser avaliado por seu potencial de risco cibernético. Alterações não autorizadas na configuração podem ser usadas como um indicador de um ataque malicioso, que pode levar à introdução de ransomware. |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| | **PR.IP-3:** Os processos de controle de mudança de configuração estão em vigor<br><br>**ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4<br><br>**NIST SP 800-53 Rev. 5** CM-3, CM-4, SA-10 | Processos de alteração de configuração adequados podem ajudar a impor atualizações de segurança oportunas ao software, manter as configurações de segurança necessárias e desencorajar a substituição de código por produtos que contenham malware ou não atendam às políticas de gestão de acesso. |
| | **PR.IP-4:** Backups de informações são conduzidos, mantidos e testados<br><br>**ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3<br><br>**NIST SP 800-53 Rev. 5** CP-4, CP-6, CP-9 | Backups regulares mantidos e testados são essenciais para a recuperação oportuna e relativamente tranquila de eventos de ransomware. Os backups devem ser protegidos para garantir que não sejam corrompidos pelo ransomware ou excluídos pelo invasor. Os backups devem ser armazenados offline. |
| | **PR.IP-9:** Planos de resposta (Resposta a incidentes e continuidade de negócios) e planos de recuperação (Recuperação de incidentes e recuperação de desastres) estão em vigor e são gerenciados<br><br>**ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3<br><br>**NIST SP 800-53 Rev. 5** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17 | Os planos de resposta e recuperação devem incluir eventos de ransomware. Uma cópia do plano de resposta deve ser mantida offline caso o incidente elimine o acesso a cópias eletrônicas mantidas na rede de destino. Os eventos de ransomware devem ser priorizados adequadamente durante a triagem de incidentes com o objetivo de contenção imediata para evitar a propagação do ransomware. |
| | **PR.IP-10:** Os planos de resposta e recuperação são testados<br><br>**ISO/IEC 27001:2013** A.17.1.3<br><br>**NIST SP 800-53 Rev. 5** CP-4, IR-3, PM-14 | Os planos de resposta e recuperação de ransomware devem ser testados periodicamente para garantir que as suposições e processos de risco e resposta estejam atualizados em relação às ameaças de ransomware em evolução. O teste de planos de resposta e recuperação deve incluir qualquer ICS associado. Os processos precisam ser atualizados e mantidos para atender às necessidades e estruturas organizacionais em constante mudança, bem como aos novos tipos e táticas de ransomware. O teste treina as pessoas que precisarão executar o plano. |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| **Manutenção (PR.MA):** A manutenção e os reparos dos componentes de controle industrial e do sistema de informação são realizados de acordo com as políticas e procedimentos. | **PR.MA-2:** A manutenção remota de ativos organizacionais é aprovada, registrada e executada de forma a impedir o acesso não autorizado<br>**ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1<br>**NIST SP 800-53 Rev. 5** MA-4 | A manutenção remota fornece um canal de acesso a redes e tecnologia. Se ele não for gerenciado adequadamente, os criminosos podem usar esse acesso para alterar as configurações e permitir a introdução de malware. A manutenção remota de todos os componentes do sistema realizada pela organização ou seus fornecedores deve ser validada para garantir que esse processo não forneça acesso ilegal às redes OT ou TI. |
| **Tecnologia de proteção (PR.PT):** As soluções de segurança técnica são gerenciadas para garantir a segurança e a resiliência dos sistemas e ativos, de acordo com as políticas, procedimentos e acordos relacionados. | **PR.PT-1:** Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política<br>**ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1<br>**NIST SP 800-53 Rev. 5** AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-12, AU-13, AU-14, AU-16 | A disponibilidade de registros de auditoria/log pode auxiliar na detecção de comportamentos inesperados e atender a processos de resposta e recuperação forenses. |
| | **PR.PT-3:** O princípio da menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais<br>**ISO/IEC 27001:2013** A.9.1.2<br>**NIST SP 800-53 Rev. 5** AC-3, CM-7 | Manter o princípio da menor funcionalidade pode impedir o movimento entre os sistemas que podem ser afetados (por exemplo, ter acesso a um sistema de controle de processo operacional a partir de uma rede administrativa). |
| **Detecção** | | |
| **Anomalias e eventos (DE.AE):** Atividade anômala é detectada e o impacto potencial dos eventos é compreendido. | **DE.AE-3:** Os dados do evento são coletados e correlacionados de várias fontes e sensores<br>**ISO/IEC 27001:2013** A.12.4.1, A.16.1.7<br>**NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 | Várias fontes e sensores, juntamente com uma solução de Gerenciamento de informações e eventos de segurança (SIEM) melhoram a visibilidade da rede, auxiliam na detecção precoce de ransomware e ajudam a entender como o ransomware pode se propagar pela rede. |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| | **DE.AE-4:** O impacto dos eventos é determinado<br>**ISO/IEC 27001:2013** A.16.1.4<br>**NIST SP 800-53 Rev. 5** CP-2, IR-4, RA-3, SI-4 | Determinar o impacto dos eventos pode informar as prioridades de resposta e recuperação para um ataque de ransomware. |
| **Monitoramento contínuo de segurança (DE.CM):** O sistema de informação e os ativos são monitorados para identificar eventos de segurança cibernética e verificar a eficácia das medidas de proteção. | **DE.CM-1:** A rede é monitorada para detectar possíveis eventos de segurança cibernética<br>**NIST SP 800-53 Rev. 5** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 | O monitoramento de rede pode detectar invasões e iniciar ações de proteção antes que códigos maliciosos possam ser inseridos ou grandes volumes de informações sejam criptografados e exfiltrados. |
| | **DE.CM-3:** A atividade do pessoal é monitorada para detectar possíveis eventos de segurança cibernética<br>**ISO/IEC 27001:2013** A.12.4.1, A.12.4.3<br>**NIST SP 800-53 Rev. 5** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 | O monitoramento da atividade do pessoal pode detectar ameaças internas ou práticas inseguras da equipe ou credenciais comprometidas e impedir possíveis eventos de ransomware. |
| | **DE.CM-4:** Código malicioso foi detectado<br>**ISO/IEC 27001:2013** A.12.2.1<br>**NIST SP 800-53 Rev. 5** SI-3, SI-8 | A detecção pode indicar que um evento de ransomware está ocorrendo ou pode estar prestes a ocorrer. O código malicioso geralmente não é executado imediatamente, portanto, pode haver tempo entre a inserção do código malicioso e sua ativação para detectá-lo antes que o ataque de ransomware seja executado. |
| | **DE.CM-7:** O monitoramento de pessoal não autorizado, conexões, dispositivos e software é realizado<br>**ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1<br>**NIST SP 800-53 Rev. 5** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 | Pessoas, conexões, dispositivos e software não autorizados são recursos em potencial para iniciar um ataque de ransomware. O monitoramento pode detectar muitos ataques de ransomware antes de serem executados. |
| | **DE.CM-8:** As verificações de vulnerabilidade são executadas<br>**ISO/IEC 27001:2013** A.12.6.1<br>**NIST SP 800-53 Rev. 5** RA-5 | As vulnerabilidades podem ser exploradas durante um ataque de ransomware. As verificações regulares podem permitir que uma organização detecte e mitigue a maioria das vulnerabilidades antes de serem usadas para executar o ransomware. |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| **Processos de detecção (DE.DP):** Os processos e procedimentos de detecção são mantidos e testados para garantir a percepção de eventos anômalos. | **DE.DP-1:** As funções e responsabilidades pela detecção são bem definidas para garantir a responsabilidade<br>**ISO/IEC 27001:2013** A.6.1.1, A.7.2.2<br>**NIST SP 800-53 Rev. 5** CA-2, CA-7, PM-14 | A compreensão clara das funções e responsabilidades é fundamental para a prestação de contas e incentiva a adesão às políticas e procedimentos organizacionais para ajudar a detectar ataques de ransomware. |
| | **DE.DP-2:** As atividades de detecção cumprem todos os requisitos aplicáveis<br>**ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3<br>**NIST SP 800-53 Rev. 5** AC-25, CA-2, CA-7, PM-14, SI-4, SR-9 | As atividades de detecção devem ser conduzidas de acordo com a política e os procedimentos da organização. |
| | **DE.DP-3:** Os processos de detecção são testados<br>**ISO/IEC 27001:2013** A.14.2.8<br>**NIST SP 800-53 Rev. 5** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 | O teste fornece a garantia de processos de detecção corretos para ataques baseados em ransomware, reconhecendo que nem todas as tentativas de invasão serão detectadas. O teste treina as pessoas que precisarão executar o plano. |
| | **DE.DP-4:** As informações de detecção de eventos são comunicadas<br>**ISO/IEC 27001:2013** A.16.1.2, A.16.1.3<br>**NIST SP 800-53 Rev. 5** AU-6, CA-2, CA-7, RA-5, SI-4 | A comunicação oportuna de eventos anômalos é necessária para poder tomar ações corretivas antes que um ataque de ransomware possa ser totalmente realizado. |
| | **DE.DP-5:** Os processos de detecção são continuamente aprimorados<br>**ISO/IEC 27001:2013** A.16.1.6<br>**NIST SP 800-53 Rev. 5** CA-2, CA-7, PL-2, PM-14, RA-5, SI-4 | As táticas usadas nos ataques de ransomware estão sendo continuamente refinadas, portanto, os processos de detecção devem evoluir continuamente para acompanhar as novas ameaças. |
| **Resposta** | | |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| **Planejamento de resposta (RS.RP):** Os processos e procedimentos de resposta são executados e mantidos para garantir a resposta aos incidentes de segurança cibernética detectados. | **RS.RP-1:** O plano de resposta é executado durante ou depois de um incidente<br>**ISO/IEC 27001:2013** A.16.1.5<br>**NIST SP 800-53 Rev. 5** CP-2, CP-10, IR-4, IR-8 | A execução imediata dos componentes de resposta de relações públicas e comunicações do plano de resposta é necessária para impedir qualquer corrupção ou exfiltração contínua de dados, conter a propagação de uma infecção para outros sistemas e redes e iniciar mensagens preventivas para minimizar mais danos, incluindo danos à reputação ou legais. |
| **Comunicações (RS.CO):** As atividades de resposta são coordenadas com as partes interessadas internas e externas (por exemplo, atendimento de agências de aplicação da lei). | **RS.CO-1:** O pessoal conhece a função de cada um e a ordem de operações quando uma resposta é necessária<br>**ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1<br>**NIST SP 800-53 Rev. 5** CP-2, CP-3, IR-3, IR-8 | A resposta a eventos de ransomware inclui respostas técnicas e de negócios. Uma resposta eficaz e eficiente requer que todas as partes compreendam suas funções e responsabilidades. As funções de resposta às comunicações devem ser formalmente documentadas nos planos de resposta e recuperação a incidentes e devem ser reforçadas pelo exercício dos planos. |
| | **RS.CO-2:** Os incidentes são relatados de acordo com os critérios estabelecidos<br>**ISO/IEC 27001:2013** A.6.1.3, A.16.1.2<br>**NIST SP 800-53 Rev. 5** AU-6, IR-6, IR-8 | A resposta a eventos de ransomware inclui respostas técnicas e de negócios. Uma resposta eficaz e eficiente requer critérios pré-estabelecidos para notificação e adesão a esses critérios durante um evento. |
| | **RS.CO-3:** As informações são compartilhadas de forma consistente com os planos de resposta<br>**ISO/IEC 27001:2013** A.16.1.2, Cláusula 7.4, Cláusula 16.1.2<br>**NIST SP 800-53 Rev. 5** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 | As prioridades de compartilhamento de informações incluem impedir a propagação de uma infecção para outros sistemas e redes, bem como mensagens preventivas. |
| | **RS.CO-4:** A coordenação com as partes interessadas ocorre de forma consistente com os planos de resposta<br>**ISO/IEC 27001:2013** Cláusula 7.4<br>**NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8 | A coordenação com as principais partes interessadas internas e externas é importante para prioridades, como conter a disseminação de desinformação e estabelecer mensagens preventivas. |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| | **RS.CO-5:** O compartilhamento voluntário de informações ocorre com partes interessadas externas para alcançar uma conscientização situacional de segurança cibernética mais ampla<br>**ISO/IEC 27001:2013** A.6.1.4<br>**NIST SP 800-53 Rev. 5** PM-15, SI-5 | O compartilhamento de informações pode gerar benefícios forenses e reduzir o impacto e a lucratividade dos ataques de ransomware. O compartilhamento voluntário deve complementar quaisquer requisitos regulamentares ou de conformidade para relatórios e compartilhamento. |
| **Análise (RS.AN):** A análise é conduzida para garantir uma resposta eficaz e atender às atividades de recuperação. | **RS.AN-1:** As notificações dos sistemas de detecção são investigadas<br>**ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5<br>**NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4 | As notificações dos sistemas de detecção devem ser pronta e totalmente investigadas, pois muitas vezes indicam um ataque de ransomware em seus estágios iniciais, que pode ser então antecipado ou ter seus impactos mitigados. |
| | **RS.AN-2:** O impacto do incidente é compreendido<br>**ISO/IEC 27001:2013** A.16.1.4, A.16.1.6<br>**NIST SP 800-53 Rev. 5** CP-2, IR-4 | A compreensão do impacto moldará a implementação do plano de recuperação. As organizações devem procurar entender o impacto técnico de um ataque de ransomware (por exemplo, quais sistemas estão indisponíveis) para depois entender o impacto resultante nos negócios (por exemplo, quais processos de negócios não podem ser entregues). Isso ajudará a garantir que o esforço de resposta e recuperação seja devidamente priorizado e dotado de recursos e os planos de continuidade de negócios implementados nesse meio tempo. |
| | **RS.AN-3:** A investigação forense é realizada<br>**ISO/IEC 27001:2013** A.16.1.7<br>**NIST SP 800-53 Rev. 5** AU-7, IR-4 | A investigação forense ajuda a identificar a causa raiz para conter e erradicar o ataque, incluindo ações como redefinir senhas de credenciais roubadas pelo invasor, excluir malware usado pelo invasor e remover mecanismos de persistência usados pelo invasor. A investigação forense também pode informar o processo de recuperação e auxiliar nas ações de relatório e compartilhamento. |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| | **RS.AN-5:** Os processos são estabelecidos para receber, analisar e responder às vulnerabilidades divulgadas à organização provenientes de fontes internas e externas (por exemplo, testes internos, boletins de segurança ou pesquisadores de segurança)<br>**NIST SP 800-53 Rev. 5** PM-15, SI-5 | Os processos de análise podem impedir futuros ataques bem-sucedidos e a disseminação do ransomware para outros sistemas e redes. Eles também podem ajudar a restaurar a confiança entre as partes interessadas. |
| **Mitigação (RS.MI):** As atividades são realizadas para evitar a expansão de um evento, mitigar seus efeitos e resolver o incidente. | **RS.MI-1:** Os incidentes estão controlados<br>**ISO/IEC 27001:2013** A.12.2.1, A.16.1.5<br>**NIST SP 800-53 Rev. 5** IR-4 | Ações imediatas devem ser tomadas para evitar a disseminação do ransomware para outros sistemas e redes, mitigar seus efeitos e resolver o incidente. A contenção do ransomware inclui qualquer ICS associado. |
| | **RS.MI-2:** Os incidentes são mitigados<br>**ISO/IEC 27001:2013** A.12.2.1, A.16.1.5<br>**NIST SP 800-53 Rev. 5** IR-4 | Ações imediatas devem ser tomadas para isolar o ransomware de forma a minimizar a danificação de dados, impedir que a infecção se espalhe na rede e para outros sistemas e redes e minimizar o impacto na missão ou nos negócios. |
| | **RS.MI-3:** As vulnerabilidades recém-identificadas são mitigadas ou documentadas como riscos aceitos<br>**ISO/IEC 27001:2013** A.12.6.1<br>**NIST SP 800-53 Rev. 5** IR-4 | A gestão de vulnerabilidades minimiza a probabilidade de ataques de ransomware bem-sucedidos. Se as vulnerabilidades não puderem ser corrigidas ou mitigadas, documentar esse risco pelo menos permitirá sua inclusão na tomada de decisões futuras e fornecerá transparência para as partes interessadas que venham a ser afetadas por eventos de ransomware. |
| **Aprimoramentos (RS.IM):** As atividades de resposta organizacional são aprimoradas ao incorporar as lições aprendidas das atividades de detecção/resposta atuais e | **RS.IM-1:** Os planos de resposta incorporam as lições aprendidas<br>**ISO/IEC 27001:2013** A.16.1.6, Cláusula 10<br>**NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8 | Isso minimiza a probabilidade de futuros ataques de ransomware bem-sucedidos e pode ajudar a restaurar a confiança entre as partes interessadas. |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| anteriores. | **RS.IM-2:** As estratégias de resposta são atualizadas<br>**ISO/IEC 27001:2013** A.16.1.6, Cláusula 10<br>**NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8 | Isso minimiza a probabilidade de futuros ataques de ransomware bem-sucedidos e pode ajudar a restaurar a confiança entre as partes interessadas. |
| **Recuperação** | | |
| **Planejamento de recuperação (RC.RP):** Processos e procedimentos de recuperação são executados e mantidos para garantir a restauração de sistemas ou ativos afetados por incidentes de segurança cibernética. | **RC.RP-1:** O plano de recuperação é executado durante ou depois de um incidente de segurança cibernética<br>**ISO/IEC 27001:2013** A.16.1.5<br>**NIST SP 800-53 Rev. 5** CP-10, IR-4, IR-8 | Iniciar imediatamente o plano de recuperação depois de identificada a causa raiz pode reduzir as perdas. |
| **Aprimoramentos (RC.IM):** O planejamento e os processos de recuperação são aprimorados ao incorporar as lições aprendidas em atividades futuras. | **RC.IM-1:** Os planos de recuperação incorporam as lições aprendidas<br>**ISO/IEC 27001:2013** A.16.1.6, Cláusula 10<br>**NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8 | Isso minimiza a probabilidade de futuros ataques de ransomware bem-sucedidos e pode ajudar a restaurar a confiança entre as partes interessadas. |
| | **RC.IM-2:** As estratégias de recuperação são atualizadas<br>**ISO/IEC 27001:2013** A.16.1.6, Cláusula 10<br>**NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8 | Isso é necessário para manter a eficácia do planejamento de contingência para futuros ataques de ransomware. |
| **Comunicações (RC.CO):** As atividades de restauração são coordenadas com partes internas e externas (por exemplo, centros de coordenação, provedores de serviços de Internet, proprietários de sistemas atacantes, vítimas, outros CSIRT e fornecedores). | **RC.CO-1:** As relações públicas são gerenciadas<br>**ISO/IEC 27001:2013** A.6.1.4, Cláusula 7.4 | Isso minimiza o impacto nos negócios por ser aberto e transparente e restaura a confiança entre as partes interessadas. |
| | **RC.CO-2:** A reputação é reparada depois de um incidente<br>**ISO/IEC 27001:2013** Cláusula 7.4 | O reparo de reputação minimiza o impacto nos negócios e restaura a confiança entre as partes interessadas. |

| Categoria | Subcategoria e referências informativas selecionadas | Aplicação de ransomware |
|---|---|---|
| | **RC.CO-3:** As atividades de recuperação são comunicadas às partes interessadas internas e externas, bem como às equipes executivas e de gestão<br>**ISO/IEC 27001:2013** Cláusula 7.4<br>**NIST SP 800-53 Rev. 5** CP-2, IR-4 | A comunicação sobre as atividades de recuperação ajuda a minimizar o impacto nos negócios e a restaurar a confiança entre as partes interessadas. |

## Referências

[1] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[2] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) (2013) *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements* (ISO, Geneva, Switzerland). Disponível no site https://www.iso.org/isoiec-27001-information-security.html

[3] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Inclui atualizações a partir de 10 de dezembro de 2020. https://doi.org/10.6028/NIST.SP.800-53r5

## Appendix A—Recursos adicionais do NIST para ransomware

Além de outros recursos citados neste documento, o National Cybersecurity Center of Excellence (NCCoE) do NIST produziu orientações adicionais para atender à mitigação de ameaças de ransomware. Elas incluem:

- NIST Special Publication (SP) 1800-26, *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*, que aborda como uma organização pode lidar com um ataque quando ele ocorre e quais recursos ela precisa ter para detectar e responder a eventos destrutivos.
- NIST SP 1800-25, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, que aborda como uma organização pode trabalhar antes que ocorra um ataque identificando seus ativos e possíveis vulnerabilidades a fim de remediá-las e proteger esses ativos.
- NIST SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events*, que apresenta abordagens para recuperação caso um ataque de integridade de dados seja bem-sucedido.
- *Protecting Data from Ransomware and Other Data Loss Events*, um guia para provedores de serviços gerenciados usarem, manterem e testarem os arquivos de backup essenciais para a recuperação de ataques de ransomware.

O NIST tem muitos outros recursos que, embora não sejam específicos de ransomware, contêm informações importantes sobre identificação, proteção, detecção, resposta e recuperação de eventos de ransomware. Vários são destacados abaixo. Para obter uma lista mais completa de recursos, acesse o site de Proteção e resposta de ransomware do NIST em https://csrc.nist.gov/ransomware.

- Aprimoramento da segurança das tecnologias de **teletrabalho**, **acesso remoto** e **traga seu próprio dispositivo (BYOD)**:
  - Telework: Working Anytime, Anywhere project
  - NIST SP 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*
- **Correção do software** para eliminar vulnerabilidades:
  - NIST SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*
  - Critical Cybersecurity Hygiene: Patching the Enterprise project
- **Utilização da tecnologia de controle de aplicativos** para impedir a execução de ransomware:
  - NIST SP 800-167, *Guide to Application Whitelisting*
- Como encontrar orientação de nível inferior para **configurar software com segurança** e

eliminar vulnerabilidades:

  - National Checklist Program

- Como obter as **informações mais recentes sobre vulnerabilidades conhecidas**:
  - National Vulnerability Database
- **Planejamento para recuperação** de eventos de segurança cibernética:
  - NIST SP 800-184, *Guide for Cybersecurity Event Recovery*
- **Planejamento de contingência para restaurar operações** depois de uma interrupção causada por ransomware:
  - NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*
- **Como lidar com ransomware** e outros **incidentes** de malware:
  - NIST SP 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
- **Como lidar** com **incidentes** de segurança cibernética em geral:
  - NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*
- Introdução à **gestão de risco de segurança cibernética:**
  - Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide