ManageEngine

# Guia da ManageEngine para a implementação da norma de segurança da informação ISO 27001 em sua organização

# Índice


Uma breve introdução à norma ISO 27001:2022 3

Por que a ISO 27001? 4

A estrutura da norma ISO 27001:2022 5

As cláusulas da ISO 27001 5

Os controles e objetivos de controle da ISO 27001 7

O papel da ManageEngine em sua jornada de conformidade com a ISO 27001 8

Produtos da ManageEngine mapeados aos controles da ISO 27001 8

A5. Controles organizacionais 8

A6. Controles de pessoas 31

A7. Controles físicos 33

A8. Controles tecnológicos 34

Produtos da ManageEngine e os controles da ISO 27001 que eles suportam 50

Assuma o controle da sua TI 51


## Isenção de responsabilidade

# Uma breve introdução à norma ISO 27001:2022

A ISO/IEC 27001:2022 faz parte da família de normas de segurança da informação ISO/IEC 27000:2018. Essas normas fornecem às organizações um conjunto de requisitos independentes de tecnologia e baseados em risco para a implementação de um sistema de gerenciamento de segurança da informação (SGSI).

Foram desenvolvidas em conjunto pela International Standards Organization (ISO) e pela International Electrotechnical Commission (IEC).

Embora a família ISO 27000 contenha diversas normas, apenas duas delas são certificáveis:

1. **ISO/IEC 27001:2022** — Esta norma fornece os requisitos para a implementação de um SGSI.
2. **ISO/IEC 27701:2019** — Esta norma fornece os requisitos para a implementação de um sistema de gerenciamento de informações de privacidade (PIMS).

Para implementar um PIMS, as organizações precisam primeiro implementar um SGSI. Afinal, sem medidas de segurança da informação, é impossível garantir a privacidade dos dados. Se sua organização lida com informações sensíveis de qualquer tipo — PII, ePHI ou dados proprietários —, você deve buscar a certificação ISO 27001.

# Por que a ISO 27001?

Sua organização deve buscar a certificação ISO 27001 caso lide com qualquer tipo de informação sensível, como PII, ePHI ou dados proprietários.

Os requisitos e controles especificados na ISO 27001 podem ajudar sua organização a identificar riscos e implementar controles para mitigá-los. Isso fortalecerá a postura de segurança da sua organização.

A conformidade com essa norma também ajuda a aumentar a confiança dos clientes nas práticas de segurança da informação da sua organização. Alguns clientes internacionais podem, inclusive, solicitar comprovação de conformidade com a ISO 27001 como evidência de práticas sólidas de segurança da informação.

Devido à sua estrutura independente de tecnologia, essa norma pode ser facilmente mapeada para outros padrões e estruturas, como o CIS Critical Security Controls, o NIST SP-800-53 (Security and Privacy Controls for Information Systems and Organizations) e outros.

A conformidade com a ISO 27001 também pode servir como um importante passo inicial na jornada de adequação a normas de privacidade de dados, como a LGPD, CCPA e outras.

# A estrutura da norma ISO 27001:2022

A norma ISO 27001 é composta por 10 cláusulas. Destas, apenas sete possuem requisitos aplicáveis.

As cláusulas 1 a 3 definem o escopo da norma, listam as referências utilizadas e apresentam as definições dos termos usados ao longo do documento.

As cláusulas 4 a 10 detalham os requisitos sobre processos, políticas e ações que precisam ser implementados para garantir a conformidade com a norma. Cada um desses requisitos é obrigatório caso sua organização busque a certificação ISO 27001.

# Cláusulas da ISO 27001

**Cláusula 4: Contexto da organização**
Aborda o contexto em que o SGSI está sendo implementado.
É necessário documentar o que a organização faz, os requisitos das partes interessadas (internas e externas) e o escopo do SGSI. Essas informações ajudam os auditores a compreender os objetivos do sistema, permitindo uma avaliação mais eficaz.

**Cláusula 5: Liderança**
Define o papel da liderança no sucesso do SGSI. Envolve a implementação de uma política de segurança da informação, a integração dos requisitos do SGSI aos processos organizacionais e outros aspectos. Também é necessário atribuir responsabilidades pelo monitoramento e pela melhoria contínua do sistema, garantindo a conformidade com a norma.

**Cláusula 6: Planejamento**
Trata do gerenciamento de riscos na organização. A documentação deve abranger os processos de identificação, análise e tratamento de riscos (mitigar, evitar ou aceitar). Também é preciso designar responsáveis pelos riscos, que terão a função de gerenciá-los.

**Cláusula 7: Suporte**
Cobre os recursos necessários para sustentar, manter e aprimorar o SGSI. Inclui a criação, manutenção e atualização da documentação exigida pelo padrão, bem como garantir sua disponibilidade. Também requer que os colaboradores estejam cientes dos requisitos do SGSI, da sua importância e das consequências do não cumprimento.

**Cláusula 8: Operação**
Trata da implementação prática dos requisitos definidos na cláusula 6. Abrange as avaliações de risco e a aplicação do plano de tratamento dos riscos. Em conjunto, as cláusulas 6 a 8 devem resultar em um plano completo de mitigação de riscos de ponta a ponta.

**Cláusula 9: Avaliação de desempenho**
Aborda o monitoramento da eficácia do SGSI. Define o que, como, quem e quando monitorar e analisar, incluindo auditorias internas e outros requisitos de verificação e melhoria do sistema.

**Cláusula 10: Melhorias**
Trata da correção de falhas e da melhoria contínua. Exige que a organização adote ações corretivas para lidar com não conformidades e revise o SGSI para evitar recorrências. Além disso, estabelece a melhoria contínua do sistema como um requisito essencial.

# Os controles e objetivos de controle da ISO 27001

Além das 10 cláusulas mencionadas anteriormente, o anexo da norma ISO 27001 também contém 93 controles divididos em quatro categorias: controles organizacionais, controles de pessoas, controles físicos e controles tecnológicos (cláusulas 5 a 8).

Esses controles apresentam requisitos detalhados que garantem a implementação eficaz de um SGSI. Diferentemente das cláusulas mencionadas na seção anterior, não é necessário implementar todos esses controles, pois alguns podem não ser aplicáveis à sua organização.

No entanto, será necessário justificar a exclusão em um documento de declaração de aplicabilidade, que será avaliado pelo auditor da certificação. Isso garante que o auditor compreenda as razões pelas quais determinados controles não foram implementados.

Em resumo, para obter a certificação de conformidade com a norma ISO 27001, é necessário:

- Cumprir todas as cláusulas mencionadas na seção anterior.
- Implementar todos os controles aplicáveis à sua organização dentre os 93 listados na tabela A.1 do anexo A da ISO 27001.

Deixar de atender a qualquer um desses requisitos pode comprometer as chances de conquistar a certificação.

# O papel da ManageEngine em sua jornada de conformidade com a ISO 27001

O grupo de soluções de gerenciamento de TI da ManageEngine pode ajudar sua organização a atender aos diversos requisitos de controle relacionados à área de TI estabelecidos pela norma ISO 27001. Isso contribui para o desenvolvimento de um programa de gerenciamento de segurança da informação robusto e auxilia na obtenção da conformidade com outros padrões de segurança e privacidade.

## Produtos da ManageEngine mapeados aos controles da ISO 27001

Mapeamos os produtos da ManageEngine aos controles da ISO 27001 que eles podem ajudar você a implementar.

### A.5 Controles organizacionais

| Controle | Definição/requisitos do controle | Produto(s) da ManageEngine que podem ajudar |
|---|---|---|
| 5.7 Inteligência de ameaças | As informações relacionadas a ameaças à segurança da informação devem ser coletadas e analisadas para gerar inteligência de ameaças. | **Log360:** Integre e colete informações de feeds e serviços de inteligência sobre ameaças.<br><br>**Endpoint Central:** Implemente um gerenciamento de vulnerabilidades abrangente com avaliação e visibilidade contínuas das ameaças a partir de um console central. Utilize a correção integrada para resolver vulnerabilidades detectadas. Garanta aplicação de patches sem interrupções em Windows, Mac, Linux e mais de 850 aplicações de terceiros, além de gerenciar atualizações para Windows, iOS, Android, ChromeOS, firmware e aplicações móveis. |

| | | |
|---|---|---|
| 5.9 Inventário de informações e outros ativos associados | Deve ser desenvolvido e mantido um inventário de informações e outros ativos associados, incluindo seus responsáveis. | **ServiceDesk Plus ou AssetExplorer:** Descubra e identifique todos os ativos de TI e não TI usando vários métodos de descoberta, como varreduras de domínio, varreduras de rede, scripts de autoexploração e varreduras baseadas em agente. Classifique os ativos, atribua responsáveis e consolide-os em um repositório centralizado para garantir visibilidade completa. Implemente práticas de gerenciamento de ativos com certificação ITIL para manter o inventário preciso e atualizado.<br><br>**Endpoint Central:** Mantenha um inventário de todos os endpoints (incluindo dispositivos móveis) e ativos de software, gerenciando-os a partir de um console central.<br><br>**Log360:** Mantenha um inventário dos softwares instalados nos endpoints, acompanhe os detalhes de propriedade e garanta que todos os ativos organizacionais estejam contabilizados e gerenciados de forma eficaz.<br><br>**OpManager Plus:** Gerencie um inventário abrangente da infraestrutura de rede e monitore sua integridade, disponibilidade e desempenho em tempo real. |

| | | |
|---|---|---|
| | | **Site24x7:** Use a ferramenta de descoberta de rede para criar um inventário preciso de toda a rede, identificando automaticamente todos os dispositivos e conexões.<br><br>**PAM360:** Descubra todos os endpoints junto com suas contas locais para consolidar, rotacionar certificados e gerenciar credenciais de identidade privilegiadas, como senhas, chaves SSH e certificados TLS.<br><br>**DataSecurity Plus:** Localize, analise e rastreie dados pessoais sensíveis, também conhecidos como PII ou ePHI, armazenados em servidores de arquivos Windows, no Microsoft SQL Server e em clusters de failover.<br><br>**AppCreator:** Crie um repositório de informações com o inventário e outros ativos associados, incluindo seus responsáveis.<br><br>**Analytics Plus:** Obtenha uma visão completa de cada endpoint, ativo e dispositivo a partir de dashboards de inventário consolidados. |

| | | |
|---|---|---|
| 5.11 Devolução de ativos | Os colaboradores e outras partes interessadas, conforme aplicável, devem devolver todos os ativos da organização sob sua posse ao encerrar ou alterar o vínculo empregatício, contratual ou de parceria. | **ServiceDesk Plus ou AssetExplorer:** Garanta a devolução dos ativos organizacionais com o suporte de um database de inventário que atua como uma única fonte de verdade para todos os ativos. Use workflows predefinidos para rastrear a devolução de ativos e acionar notificações automáticas caso um ativo seja marcado como perdido. Automatize aprovações para garantir conformidade durante o offboarding.<br><br>**Endpoint Central:** Garanta total visibilidade sobre os ativos de endpoint com dashboards intuitivos e relatórios prontos para uso.<br><br>**Log360:** Monitore alterações em contas de usuários para garantir que colaboradores desligados não mantenham acesso. Acompanhe softwares instalados para verificar e recuperar ativos fornecidos pela organização e assegure que dados críticos sejam arquivados com segurança antes do desligamento para evitar perda de informações.<br><br>**PAM360:** Revogue automaticamente o acesso privilegiado a endpoints concedido a usuários que mudaram de equipe/departamento ou encerraram seu empregatício, contratual ou de parceria com a organização. |

| | | |
|---|---|---|
| | | Rotacione todas as senhas e chaves SSH usadas recentemente para acesso privilegiado.<br><br>**DataSecurity Plus:** Localize, analise e rastreie dados pessoais sensíveis, também conhecidos como PII ou ePHI, armazenados em servidores de arquivos Windows, no Microsoft SQL Server e em clusters de failover.<br><br>**AppCreator:** Crie um repositório de gerenciamento de ativos e rastreie-os desde a aquisição e alocação até a desativação.<br><br>**Analytics Plus:** Consolide dados de RH e inventário de ativos. Durante mudanças de pessoal, receba alertas automáticos para rastrear e garantir a devolução de ativos e dispositivos atribuídos. |
| 5.12 Classificação da informação | As informações devem ser classificadas conforme as necessidades de segurança da informação da organização, com base em confidencialidade, integridade, disponibilidade e nos requisitos das partes interessadas relevantes. | **Data Security Plus:** Localize, analise e rastreie dados pessoais sensíveis, também conhecidos como PII ou ePHI, armazenados em servidores de arquivos Windows, no Microsoft SQL Server e em clusters de failover.<br><br>**Endpoint Central:** Permita que os administradores de TI descubram e classifiquem vários tipos de dados estruturados e não estruturados usando mecanismos avançados, como identificação por impressão digital, RegEx, filtros baseados em extensão de arquivo e pesquisa por palavras-chave. |

| | | |
|---|---|---|
| 5.13 Rotulagem da informação | Um conjunto adequado de procedimentos para rotulagem da informação deve ser desenvolvido e implementado de acordo com o esquema de classificação adotado pela organização. | **Endpoint Central:** Localize, analise e rastreie dados pessoais sensíveis, também conhecidos como PII ou ePHI, armazenados em suas redes. |
| 5.14 Transferência de informações | Regras, procedimentos ou acordos para transferência de informações devem ser definidos e aplicados para todos os tipos de meios de transferência, tanto dentro da organização quanto entre a organização e outras partes. | **Log360:** Monitore transferências de arquivos, acessos de usuários e eventos do sistema em ambientes on-premises e em cloud para garantir trocas de informações seguras. |

| | | |
|---|---|---|
| 5.15 Controle de acesso | Devem ser estabelecidas e implementadas regras para controlar o acesso físico e lógico às informações e outros ativos associados, com base nos requisitos de segurança da informação e das necessidades de negócio. | **AD360:** Configure regras de MFA com base no IP do usuário, geolocalização, horário de acesso e dispositivo utilizado, restringindo ou permitindo o acesso a informações e ativos conforme necessário. Revise e verifique periodicamente o acesso de usuários aos recursos organizacionais por meio de campanhas de certificação de acesso.<br><br>**Identity360:** Defina permissões e funções automatizadas e granulares conforme os usuários se movimentam dentro da organização. Proteja os recursos garantindo que usuários específicos tenham os devidos privilégios.<br><br>**ServiceDesk Plus:** Receba, autorize e administre solicitações de provisionamento de acesso utilizando recursos de gerenciamento de solicitações com certificação ITIL. Unifique serviços em um catálogo centralizado e disponibilize-os para grupos específicos de colaboradores conforme suas funções. Implemente verificações detalhadas por meio de workflows visuais com aprovações em vários níveis. Gerencie o provisionamento de acesso por meio de automações de workflow simplificadas, acionadas por eventos como aprovações. |

| | | |
|---|---|---|
| | | **PAM360:** Aplique controles de acesso com base em Zero Trust, impondo workflows de solicitação e liberação de senhas que exigem aprovação de administradores para cada solicitação de acesso remoto. Atribua pontuações de confiança a cada usuário e endpoint, com base em condições como endereço IP, horário de login e plug-ins do navegador instalados. Crie políticas de acesso baseadas nessas pontuações para negar acesso a endpoints caso o valor fique abaixo do limite pré-definido, garantindo controle de acesso baseado em políticas.<br><br>**Log360:** Aplique controles de acesso monitorando logons de usuários, atividades de sessão e tentativas de autenticação em ambientes on-premises e em cloud. Acompanhe alterações em contas, tentativas de acesso falhas e políticas de acesso condicional para detectar acessos não autorizados, garantir conformidade e fortalecer controles de segurança. |

| | | |
|---|---|---|
| | | **Endpoint Central:** Utilize o gerenciamento de privilégios de endpoint para aplicar o princípio do privilégio mínimo.<br>Ative gerenciamento de privilégios específico por aplicação e acesso just-in-time para os usuários finais.<br>Liste ou bloqueie aplicações em endpoints críticos usando o módulo de controle de aplicações. Implemente políticas de acesso condicional para validar usuários autorizados a acessar sistemas e dados críticos dos negócios.<br><br>**OpManager Plus:** Utilize controle de acesso baseado em função para garantir que os usuários só possam acessar os dispositivos atribuídos pelos administradores, enviando automaticamente solicitações de aprovação quando forem feitas alterações nesses dispositivos.<br><br>**AppCreator:** Aplique controles de acesso granulares e baseados em regras para aplicações personalizadas do setor de assistência médica e cuidados de saúde desenvolvidas no AppCreator. Estenda esses controles de acesso a aplicações de terceiros integradas às suas aplicações personalizadas. |

| | | |
|---|---|---|
| 5.16 Gerenciamento de identidades | O ciclo de vida completo das identidades deve ser gerenciado. | **AD360 ou Identity360:** Simplifique o gerenciamento do ciclo de vida de identidades com provisionamento em massa de usuários em várias plataformas, automação, templates personalizáveis e integração com sistemas de gerenciamento de capital humano. |
| 5.17 Informações de autenticação | A alocação e o controle das informações de autenticação devem ser controlados por um processo de gerenciamento, incluindo a orientação dos colaboradores sobre o tratamento adequado dessas informações. | **AD360:** Simplifique o gerenciamento de senhas para administradores de TI e reduza a dependência do help desk para os usuários finais com gerenciamento de autoatendimento de senhas, políticas de senha robustas, sincronização de senhas e notificações de expiração de senhas.<br><br>**Log360:** Acompanhe mudanças em contas de usuários e detalhes de autenticação em sistemas e databases. Monitore tentativas de login e garanta o controle adequado de informações de autenticação, como senhas, para evitar acessos não autorizados.<br><br>**Endpoint Central:** Defina políticas de código de acesso para dispositivos móveis com Android, Apple e Windows, garantindo que os usuários criem códigos fortes para seus dispositivos. Use essas políticas para configurar o número máximo de tentativas de código incorretas, o tempo máximo de inatividade permitido antes do bloqueio automático e outras configurações. |

| | | |
|---|---|---|
| 5.18<br>Direitos de acesso | Os direitos de acesso a informações e outros ativos associados devem ser provisionados, revisados, modificados e removidos de acordo com a política específica da organização e as regras de controle de acesso. | **AD360:** Revise e verifique periodicamente o acesso de usuários aos recursos organizacionais por meio de campanhas de certificação de acesso.<br><br>**Identity360:** Automatize a atualização de funções e permissões conforme os usuários mudam de cargo, protegendo os recursos com privilégios precisos.<br><br>**PAM360:** Aplique o princípio do privilégio mínimo em todos os endpoints por meio de controles de acesso baseados em função e em políticas, limitando a visibilidade de usuários remotos conforme os requisitos de segurança da informação da organização.<br><br>**ServiceDesk Plus:** Habilite e gerencie modificações de acesso por meio de formulários de solicitação detalhados. Colete informações precisas por meio dos campos do template sempre que uma modificação de direitos de acesso for solicitada. Gerencie a governança de acesso com aprovações em múltiplos níveis.<br><br>**OpManager Plus:** Utilize RBAC para restringir o acesso de usuários a ativos sujeitos a alterações de configuração. Além disso, todas as alterações realizadas nesses ativos são automaticamente enviadas aos administradores para aprovação. |

| | | |
|---|---|---|
| | | **Log360:** Monitore alterações em contas de usuários, modificações em grupos e atividades de login para garantir que os direitos de acesso estejam alinhados com as políticas organizacionais. Acompanhe o acesso a databases e dispositivos de rede para evitar uso não autorizado.<br><br>**Endpoint Central:** Utilize o gerenciamento de privilégios de endpoint para aplicar o princípio do privilégio mínimo. Ative gerenciamento de privilégios específico por aplicação e acesso just-in-time para os usuários finais. Liste ou bloqueie aplicações em endpoints críticos usando o módulo de controle de aplicações. Implemente políticas de acesso condicional para validar usuários autorizados a acessar sistemas e dados críticos dos negócios.<br><br>**AppCreator:** Aplique controles de acesso granulares e baseados em regras para aplicações personalizadas do setor de assistência médica e cuidados de saúde desenvolvidas no AppCreator. |

| | | |
|---|---|---|
| 5.19 Segurança da informação no relacionamento com fornecedores | Devem ser definidos e implementados processos e procedimentos para gerenciar os riscos à segurança da informação associados ao uso de produtos ou serviços de fornecedores. | **ServiceDesk Plus:** Crie módulos personalizados para gerenciar avaliações de risco de fornecedores. Inclua nesses módulos campos que permitam registrar e categorizar riscos. Inicie ações de mitigação, como notificação de partes interessadas e criação de tickets, por meio de automações low-code. |
| 5.21 Gerenciamento da segurança da informação na cadeia de fornecimento de TIC | Processos e procedimentos devem ser definidos e implementados para gerenciar os riscos de segurança da informação associados à cadeia de fornecimento de produtos e serviços de TIC. | **ServiceDesk Plus:** Utilize módulos personalizados e crie questionários de avaliação de risco para identificar os riscos associados aos fornecedores da cadeia de fornecimento de TIC. Acione automações personalizadas com base nos riscos identificados. |

| | | |
|---|---|---|
| 5.23 Segurança da informação no uso de serviços baseados em cloud | Devem ser estabelecidos processos para aquisição, uso, gerenciamento e descontinuação de serviços baseados em cloud, em conformidade com os requisitos de segurança da informação da organização. | **Log360:** Garanta o uso seguro da cloud auditando a atividade dos usuários, os controles de acesso e as alterações de configuração.<br><br>**Identity360:** Implemente o gerenciamento do ciclo de vida de identidades com provisionamento em massa de usuários e templates personalizáveis. Defina permissões automatizadas e granulares conforme os usuários mudam de função, simplificando o gerenciamento de acesso à cloud.<br><br>**ServiceDesk Plus:** Crie workflows visuais dedicados e otimize o processo de solicitação e aquisição de serviços em cloud. Associe e gerencie ordens de compra e contratos junto às aprovações, e acompanhe suas datas de vencimento com notificações automáticas.<br><br>**Site24x7:** Realize monitoramento de segurança abrangente de sites e aplicações web públicas, incluindo verificações de desfiguração de sites, validação de certificados SSL/TLS, avaliações de reputação da marca e verificações em listas de bloqueio em tempo real. Gere relatórios para identificar possíveis ameaças e vulnerabilidades nos seus sites. |

| | | |
|---|---|---|
| 5.24 Planejamento e preparação para o gerenciamento de incidentes de segurança da informação | A organização deve planejar e se preparar para o gerenciamento de incidentes de segurança da informação, definindo, estabelecendo e comunicando processos, papéis e responsabilidades. | **ServiceDesk Plus:** Desenvolva templates estruturados de gerenciamento de incidentes que definam funções, responsabilidades, SLAs, tarefas e procedimentos de resposta. Crie workflows predefinidos com notificações automáticas via Microsoft Teams para manter as partes interessadas informadas. Realize análises detalhadas de impacto com uma CMDB integrada para identificar ativos, serviços e dependências afetadas, acelerando a resolução. |
| 5.25 Avaliação e decisão com base em eventos de segurança da informação | A organização deve avaliar eventos de segurança da informação e decidir se eles devem ser categorizados como incidentes de segurança da informação. | **ServiceDesk Plus:** Utilize triagem com tecnologia de IA para categorizar, priorizar e direcionar com precisão os incidentes de segurança da informação para as equipes de resposta adequadas. Ative fluxos de trabalho visuais que orientem os membros das equipes de resposta na avaliação de impacto e tomada de decisões com automações integradas. |

| | | |
|---|---|---|
| 5.26 Resposta a incidentes de segurança da informação | Os incidentes de segurança da informação devem ser tratados de acordo com os procedimentos documentados. | **Log360:** Identifique incidentes de segurança por meio da análise de eventos do sistema, monitore a atividade de firewall para detectar conexões suspeitas e analise dados de ameaças para garantir resposta e mitigação em tempo hábil, conforme os procedimentos documentados. Além disso, automatize respostas e resoluções de primeiro nível para incidentes comuns usando workflows automáticos. Esses fluxos podem acionar ações predefinidas, como desativar contas comprometidas, bloquear IPs suspeitos ou notificar as equipes de segurança em tempo real, garantindo contenção rápida e reduzindo a necessidade de intervenção manual.<br><br>**ServiceDesk Plus:** Colete evidências por meio de campos pré-configurados e campos personalizados de ticket ao longo do processo de resposta a incidentes. Estabeleça procedimentos operacionais padrão (POP) e conduza a governança com workflows de resposta a incidentes pré-configurados. Realize análises detalhadas de causa raiz (RCA) e trate as causas subjacentes com um módulo de gerenciamento de problemas totalmente integrado. |

| | | |
|---|---|---|
| 5.27 Aprendizado com incidentes de segurança da informação | O conhecimento adquirido a partir de incidentes de segurança da informação deve ser utilizado para fortalecer e aprimorar os controles de segurança da informação. | **ServiceDesk Plus:** Gere análises detalhadas pós-incidente com os recursos de IA generativa da Zia. Resuma conversas dentro dos tickets para melhorar o entendimento do contexto. Transfira esses resumos e insights como notas para comunicar claramente o histórico dos incidentes. Documente a resolução em um repositório central de conhecimento para estabelecer POPs e reduzir o impacto de incidentes futuros. |
| 5.28 Coleta de evidências | A organização deve estabelecer e implementar procedimentos para identificação, coleta, aquisição e preservação de evidências relacionadas a eventos de segurança da informação. | **Log360:** Capture e preserve dados críticos de eventos de segurança auditando logins, atividade de firewall, alterações em arquivos e rastreamento de processos em sistemas, databases e ambientes em cloud. Garanta a prontidão pericial coletando evidências sobre logins malsucedidos, uso de discos removíveis e anomalias no tráfego de rede.<br><br>**Endpoint Central:** Em caso de evento suspeito registrado na rede de TI, registre e encaminhe detalhes do ataque e dos endpoints envolvidos ao administrador de rede ou à equipe do SOC.<br><br>**ServiceDesk Plus:** Garanta a coleta diligente de evidências por meio de campos predefinidos e personalizados nos tickets durante o processo de resposta a incidentes e outras práticas de ITSM. Gere análises pós-incidente com o GenAI. |

| | | |
|---|---|---|
| | | Estabeleça POPs e playbooks para coleta de evidências utilizando workflows visuais, nos quais os campos são obrigatórios e as partes interessadas são notificadas.<br><br>**PAM360:** Audite todos os registros de acessos privilegiados com detalhes sobre "quem", "quando", "onde" e "para qual finalidade" o acesso foi concedido. Registre todas as atividades executadas pelos usuários em sessões remotas privilegiadas para fins de investigação e revisão de acesso. |
| 5.30 Prontidão de TIC para a continuidade dos negócios | A prontidão de TIC deve ser planejada, implementada, mantida e testada com base nos objetivos de continuidade dos negócios e nos requisitos de continuidade de TIC. | **Endpoint Central:** Utilize o mecanismo de antivírus de nova geração (NGAV) para garantir defesa proativa contra ameaças cibernéticas, como malwares, com detecção comportamental em tempo real assistida por IA e tecnologia de aprendizado profundo. Aproveite os recursos de análise pericial de incidentes da plataforma para identificar a causa raiz e a gravidade das ameaças. Isole automaticamente endpoints afetados usando o módulo NGAV quando comportamentos suspeitos ou malwares forem detectados e, após a análise pericial e correção, retorne-os ao ambiente de produção. Utilize backups não apagáveis de arquivos, capturados a cada três horas com o serviço de cópias de sombra da Microsoft, para restaurar instantaneamente arquivos criptografados por ransomware. |

| | | |
|---|---|---|
| 5.31 Requisitos legais, estatutários, regulatórios e contratuais | Devem ser identificados, documentados e mantidos atualizados os requisitos legais, estatutários, regulatórios e contratuais relevantes à segurança da informação, bem como a abordagem da organização para cumpri-los. | **ServiceDesk Plus:** Garanta a conformidade identificando, documentando e atualizando regularmente artigos de conhecimento sobre requisitos legais, estatutários, regulatórios e contratuais. Incorpore esses artigos ao portal de autoatendimento para facilitar o acesso dos colaboradores às orientações e requisitos aplicáveis.<br><br>**Log360:** Utilize relatórios integrados para identificar e documentar requisitos legais e contratuais. Garanta o monitoramento contínuo e mantenha registros precisos para otimizar auditorias e avaliações regulatórias.<br><br>**Endpoint Central:** Implemente os controles necessários em endpoints e gere relatórios prontos para auditoria, assegurando conformidade com normas globais e regionais de privacidade de dados e segurança da informação, como a LGPD, CIS Critical Security Controls, NIST Cybersecurity Framework e outros.<br><br>**OpManager Plus:** Utilize o módulo de gerenciamento de configuração para garantir conformidade com padrões como CIS Benchmarks, PCI DSS, SOX e HIPAA. Para requisitos adicionais, defina políticas personalizadas configurando suas próprias regras. |

| | | |
|---|---|---|
| | | Além disso, regras em desconformidade podem ser automaticamente corrigidas.<br><br>**Nota:** As soluções da ManageEngine podem ajudar organizações como a sua a cumprir diversos regulamentos e padrões de privacidade e segurança da informação regionais e globais, como o LGPD, os Controles de Segurança Críticos do CIS, o NIST Cybersecurity Framework e outros. Acesse esta página para saber mais. |
| 5.32<br>Direitos de propriedade intelectual | A organização deve implementar procedimentos adequados para proteger os direitos de propriedade intelectual. | **Endpoint Central:** Localize, analise e rastreie informações sensíveis, como patentes, contratos e outros arquivos confidenciais armazenados nas suas redes.<br><br>**Analytics Plus:** Identifique e categorize instalações de softwares não autorizados com base em risco e conformidade. Analise tendências de uso para fornecer alternativas mais seguras quando necessário e evitar o ressurgimento de shadow IT. |

| | | |
|---|---|---|
| 5.33 Proteção de registros | Os registros devem ser protegidos contra perda, destruição, falsificação, acesso não autorizado e divulgação indevida. | **AD360:** Faça backups periódicos dos dados no Active Directory (AD), Microsoft 365, Google Workspace e Exchange Server, armazenando-os de forma segura como múltiplas versões criptografadas, garantindo a restauração em caso de perda de dados. Proteja os registros contra acesso não autorizado utilizando métodos robustos de MFA.<br><br>**PAM360:** Aplique workflows de aprovação administrativa para solicitações de acesso remoto a endpoints com registros confidenciais.<br><br>**Endpoint Central:** Aplique controles para evitar vazamento de dados corporativos por meio de dispositivos periféricos, upload em clouds públicas, impressão de páginas da web e uso da área de transferência. Implemente políticas de acesso condicional para validar o acesso de usuários autorizados a sistemas e dados críticos dos negócios. |

| | | |
|---|---|---|
| 5.34 Privacidade e proteção de PII | A organização deve identificar e atender aos requisitos relacionados à preservação da privacidade e à proteção de informações pessoais identificáveis (PII) conforme as leis, regulamentações e exigências contratuais aplicáveis. | **ServiceDesk Plus:** Dentro das solicitações de TI e corporativas recebidas, criptografe os campos que contêm PII para proteger as informações pessoais dos solicitantes. Configure as opções de privacidade no ServiceDesk Plus para anonimizar e excluir os dados da aplicação quando necessário.<br><br>**AD360 ou Identity360:** Proteja PII com métodos modernos de MFA resistentes a phishing, garantindo conformidade com normas como PCI DSS, HIPAA, LGPD e NIS2.<br><br>**Endpoint Central:** Localize, analise e rastreie dados pessoais sensíveis, também conhecidos como PII ou ePHI, armazenados em suas redes. Aplique controles sobre o compartilhamento de arquivos e o uso de dispositivos periféricos para evitar vazamento de dados por meio de unidades USB, impressoras, uploads de arquivos para a cloud pública e outros vetores.<br><br>**AppCreator:** Criptografe dados pessoais, como PII ou ePHI, registrados em aplicações personalizadas de assistência médica e cuidados de saúde criadas no AppCreator para garantir a proteção e privacidade das informações.<br><br>**OpManager Plus:** Localize e identifique PII armazenadas nos diferentes módulos do OpManager Plus. |

| | | |
|---|---|---|
| 5.36 Conformidade com políticas, regras e padrões de segurança da informação | A conformidade com a política de segurança da informação da organização, políticas específicas por tema, regras e padrões deve ser revisada regularmente. | **AD360:** Utilize relatórios predefinidos para revisar e identificar possíveis desvios de conformidade em relação a regulamentações e padrões.<br><br>**ServiceDesk Plus:** Documente e gerencie as políticas e regras de segurança da informação da organização como artigos de conhecimento em um repositório central. Configure mecanismos de revisão e aprovação de documentos com controle de acesso baseado em função para manter as informações sempre atualizadas.<br><br>**Endpoint Central:** Use a geração de relatórios integrada para gerar relatórios e insights sobre o parque de endpoints da organização para fins de governança e auditoria.<br><br>**Firewall Analyzer ou OpManager Plus:** Simplifique auditorias de conformidade de firewall com os recursos integrados de gerenciamento de conformidade do Firewall Analyzer, que oferecem relatórios prontos alinhados a normas como PCI DSS, ISO 27001, NIST, SANS, NERC-CIP, SOX, LGPD, GLBA, HIPAA e mais. |

## A.6 Controles de pessoas

| Controle | Definição/requisitos do controle | Produto(s) da ManageEngine que podem ajudar |
|---|---|---|
| 6.7 Trabalho remoto | Devem ser implementadas medidas de segurança quando colaboradores estiverem trabalhando remotamente, a fim de proteger as informações acessadas, processadas ou armazenadas fora das instalações da organização. | **Endpoint Central:** Utilize protocolos de Padrão de Criptografia Avançada (AES) de 256 bits durante operações remotas para soluções de problemas. Execute os endpoints no modo FIPS para garantir operações seguras e protegidas.<br><br>**PAM360:** Aplique workflows de aprovação administrativa para solicitações de acesso remoto. Associe pontuações de confiança a usuários e dispositivos remotos com base em tentativas de login inválidas, logins fora do horário comercial, plug-ins de navegador instalados, autenticação de dois fatores, entre outros fatores. Crie políticas de acesso e mapeie-as para endpoints privilegiados, analisando solicitações de acesso de usuários remotos com pontuações de confiança que não atendam aos padrões organizacionais.<br><br>**AD360:** Proteja sessões de acesso remoto com MFA, tanto no cliente quanto no dispositivo de destino, utilizando autenticadores fortes. |

| | | |
|---|---|---|
| | | **Analytics Plus:** Crie dashboards consolidados para proteger todos os aspectos do trabalho remoto a partir de uma única interface. Avalie a conformidade de patches dos ativos, identifique instalações de shadow IT, senhas fracas, contas inativas e outros pontos de vulnerabilidade para aprimorar as práticas de segurança de forma integrada. |
| 6.8 Relatório de evento de segurança da informação | A organização deve prover um mecanismo para reportar eventos de se de segurança da informação observados ou suspeitos por meio dos canais adequados, em tempo hábil. | **ServiceDesk Plus:** Utilize um sistema omnicanal de registro de incidentes integrado a diversas ferramentas de monitoramento de TI, UEM, SIEM e colaboração. Após o registro do ticket, realize a triagem, o gerenciamento e a resolução dos incidentes por meio de workflows totalmente automatizados e com suporte de IA. |

## A.7 Controles físicos

| Controle | Definição/requisitos do controle | Produto(s) da ManageEngine que podem ajudar |
|---|---|---|
| 7.10 Mídias de armazena-mento | As mídias de armazenamento devem ser gerenciadas ao longo de todo o seu ciclo de vida, incluindo aquisição, uso, transporte e descarte, de acordo com o esquema de classificação e os requisitos de manuseio da organização. | **ServiceDesk Plus:** Classifique os ativos de TI como mídias de armazenamento, gerencie-os a partir de um repositório central e utilize workflows visuais dedicados para cada etapa do ciclo de vida do ativo, desde a aquisição até o descarte.<br>**Endpoint Central:** Utilize as capacidades de gerenciamento de dispositivos periféricos para bloquear mídias de armazenamento externas. Crie uma lista de dispositivos confiáveis que os usuários possam utilizar em seus endpoints. Use o módulo integrado de gerenciamento de ativos para rastrear mídias de armazenamento desde a aquisição até o descarte. Garanta a remoção segura de quaisquer dados corporativos ou sensíveis antes do descarte dos ativos. |
| 7.14 Descarte ou reutilização segura de equipamentos | Os equipamentos que contenham mídias de armazenamento devem ser verificados para garantir que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobrescritos com segurança antes do descarte ou reutilização. | **Endpoint Central:** Execute limpezas remotas para garantir a segurança dos dados corporativos em caso de perda de dispositivo. Restaure os dispositivos para as configurações de fábrica, permitindo que equipamentos utilizados por ex-colaboradores sejam facilmente reconfigurados pelos administradores para uso de novos colaboradores.<br>**ServiceDesk Plus:** Quando um ativo de TI atingir o fim de sua vida útil ou precisar ser descartado, notifique automaticamente as partes interessadas para garantir a remoção de quaisquer dados sensíveis ou softwares licenciados. |

## A.8 Controles tecnológicos

| Controle | Definição/requisitos do controle | Produto(s) da ManageEngine que podem ajudar |
|---|---|---|
| 8.1 Dispositivos de endpoint do usuário | As informações armazenadas, processadas ou acessadas por meio de dispositivos de endpoint do usuário devem ser protegidas. | **Endpoint Central:** Localize, analise e rastreie dados pessoais sensíveis armazenados nas suas redes. Implemente a compartimentalização de dados pessoais e corporativos para garantir a segurança das informações corporativas. Defina políticas de códigos de acesso e aplique medidas de segurança em dispositivos e navegadores para reduzir riscos. Implemente criptografia de armazenamento e controles de prevenção contra perda de dados (DLP) para evitar vazamento de informações por dispositivos periféricos, uploads para a cloud pública e outros meios.<br><br>**ServiceDesk Plus:** Identifique estações de trabalho com softwares proibidos e notifique as equipes responsáveis. Integre soluções UEM, como Endpoint Central e Microsoft Intune, para executar ações corretivas, como associação/dissociação de perfis, limpeza de dados corporativos ou geolocalização de dispositivos móveis.<br><br>**AD360 ou Identity360:** Proteja o acesso a endpoints corporativos utilizando autenticação forte e adaptável. |

| | | |
|---|---|---|
| 8.2 Direitos de acesso privilegiado | A atribuição e o uso de direitos de acesso privilegiado devem ser restritos e gerenciados. | **PAM360:** Aplique workflows de aprovação administrativa para solicitações de acesso remoto. Associe pontuações de confiança a usuários e dispositivos remotos com base em tentativas de login inválidas, logins fora do horário comercial, plug-ins de navegador instalados, autenticação de dois fatores. Implemente controle de acesso baseado em função (RBAC) para garantir que os usuários acessem apenas os recursos correspondentes às suas funções. Defina políticas de acesso e vincule-as a endpoints privilegiados para avaliar e controlar solicitações de acesso remoto com base nessas pontuações de confiança.<br><br>**Endpoint Central:** Utilize o gerenciamento de privilégios de endpoint para aplicar o princípio do privilégio mínimo. Ative gerenciamento de privilégios específico por aplicação e acesso just-in-time para os usuários finais. |
| 8.3 Restrição de acesso à informação | O acesso à informação e a outros ativos associados deve ser restrito de acordo com a política específica de controle de acesso estabelecida. | **AD360:** Restrinja o acesso a recursos utilizando regras de MFA baseadas em IP, geolocalização, horário de acesso e dispositivo utilizado. Revise e verifique periodicamente o acesso de usuários aos recursos organizacionais por meio de campanhas de certificação de acesso. |

| | | |
|---|---|---|
| | | **Identity360:** Gerencie permissões de acesso de forma eficiente por meio de sincronização automatizada de funções e gerenciamento em massa de acessos, mantendo os recursos protegidos.<br><br>**PAM360:** Controle o acesso privilegiado por meio de workflows de aprovação, elevação just-in-time e capacidades de autoelevação. Conceda privilégios de acesso com base em políticas de controle e na avaliação em tempo real do nível de risco de usuários e dispositivos.<br><br>**Endpoint Central:** Utilize o gerenciamento de privilégios de endpoint para aplicar o princípio do privilégio mínimo. Ative gerenciamento de privilégios específico por aplicação e acesso just-in-time para os usuários finais. Liste ou bloqueie aplicações em endpoints críticos usando o módulo de controle de aplicações. Implemente políticas de acesso condicional para validar usuários autorizados a acessar sistemas e dados críticos dos negócios. |

| | | |
|---|---|---|
| 8.5 Autenticação segura | Tecnologias e procedimentos de autenticação segura devem ser implementados com base nas restrições de acesso à informação e na política específica de controle de acesso. | **AD360:** Implemente MFA adaptável utilizando métodos fortes, como chaves FIDO resistentes a phishing, YubiKey e biometria. Revise e verifique periodicamente o acesso de usuários aos recursos organizacionais por meio de campanhas de certificação de acesso.<br><br>**Identity360:** Simplifique o gerenciamento de acessos com atualizações de função, garantindo que os usuários possuam os privilégios corretos e que os recursos permaneçam protegidos.<br><br>**OpManager Plus:** Controle e proteja o acesso aos componentes de rede utilizando diferentes opções de autenticação, incluindo servidor RADIUS, AD, SAML e autenticação de dois fatores.<br><br>**PAM360:** Exija aprovação administrativa para solicitações de acesso remoto. Calcule pontuações de confiança para usuários e dispositivos remotos com base em fatores predefinidos, como tentativas de login malsucedidas, logins fora do horário comercial, extensões de navegador instaladas e autenticação de dois fatores. Utilize controle de acesso baseado em função para restringir o acesso de acordo com cargos e níveis de confiança. Configure políticas de acesso e associe-as a endpoints privilegiados para avaliar e regular solicitações de acesso remoto conforme essas pontuações de confiança. |

| | | |
|---|---|---|
| | | **Endpoint Central:** Utilize o Windows Hello para dispositivos Windows e configure autenticação de dois fatores para usuários finais do Windows. Garanta acesso seguro a aplicações corporativas utilizando SSO corporativo baseado em Kerberos ou autenticação baseada em certificado via SCEP. |
| 8.6 Gerenciamento de capacidades | O uso de recursos deve ser monitorado e ajustado de acordo com os requisitos de capacidade atuais e previstos. | **OpManager Plus:** Garanta o monitoramento contínuo de armazenamento e previsão de capacidade a partir de uma interface unificada, utilizando o aprendizado de máquina (ML) interno para processar dados da rede, analisar indicadores-chave de desempenho e gerar tendências de previsão por meio de relatórios, gráficos e visualizações.<br><br>**Site24x7:** Visualize e acompanhe métricas de utilização de recursos, como CPU, memória e armazenamento, com a funcionalidade de planejamento de capacidade. Monitorar a integridade e o status dos recursos agrupados sob o monitor de capacidade, preveja e gerencie a capacidade de recursos e otimize a distribuição de carga de trabalho por meio da análise Top N/Bottom N.<br><br>**Endpoint Central:** Analise a duração de uso de softwares e o número de vezes que cada software é utilizado para tomar decisões informadas sobre compras, identificando tendências de uso máximo de ativos. |

| | | |
|---|---|---|
| | | Avalie o inventário atual de licenças de software com base nessas tendências, utilizando o módulo de gerenciamento de licenças. Acompanhe licenças de software prestes a expirar ou já expiradas.<br><br>**Analytics Plus:** Acesse inventários detalhados de ativos e recursos. Obtenha previsões precisas alinhadas às necessidades organizacionais em evolução. Execute simulações para visualizar os recursos necessários ao cumprimento das metas de negócios e identifique lacunas de capacidade. Simplifique o planejamento de capacidade de forma eficiente. |
| 8.7 Proteção contra malware | Deve ser implementada proteção contra malware, apoiada por medidas adequadas de conscientização dos usuários. | **Endpoint Central:** Aproveite o mecanismo integrado NGAV que utiliza tecnologia de aprendizado profundo e detecção comportamental em tempo real assistida por IA para detectar proativamente malwares. Conte com recursos de análise pericial de incidentes para permitir que as equipes de segurança analisem a causa raiz e a gravidade das ameaças detectadas. Isole automaticamente endpoints afetados usando o módulo NGAV quando comportamentos suspeitos ou malwares forem detectados e, após a análise pericial e correção, retorne-os ao ambiente de produção.<br><br>**AD360:** Proteja os endpoints contra ataques utilizando autenticação forte e adaptável. Faça backups regulares e armazene-os com segurança em múltiplas versões criptografadas, garantindo fácil restauração em caso de ataque. |

| | | |
|---|---|---|
| | | **Log360:** Detecte e analise ameaças de malware monitorando logs de antivírus, atividade de firewall e eventos de segurança de endpoints. Identifique arquivos suspeitos, rastreie ameaças baseadas em e-mail e fortaleça a proteção com inteligência de ameaças em tempo real em sistemas e redes. |
| 8.8 Gerenciamento de vulnerabilidades técnicas | As informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas, a exposição da organização a essas vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas. | **Endpoint Central:** Adote um gerenciamento de vulnerabilidades baseado em risco para sistemas de informação críticos e não críticos. Priorize vulnerabilidades com base em métricas como pontuação CVSS, disponibilidade de patches e outros fatores. Implemente um gerenciamento de vulnerabilidades abrangente com avaliação e visibilidade contínuas das ameaças a partir de um console central. Utilize a ferramenta de correção integrada para aplicar patches ou mitigar quaisquer vulnerabilidades identificadas em sua rede.<br><br>**OpManager Plus:** Mantenha as defesas da rede atualizadas com a mais recente inteligência de ameaças por meio do módulo de gerenciamento de configuração, que conta com recursos avançados de detecção de vulnerabilidades. As assinaturas são atualizadas diariamente com dados do National Vulnerability Database (NVD) e de fornecedores diretos. Obtenha insights sobre vulnerabilidades de dispositivos, ativos expostos e distribuição de versões para garantir proteção completa. |

| | | |
|---|---|---|
| 8.9 Gerenciamento de configuração | As configurações, incluindo as de segurança de hardware, software, serviços e redes, devem ser estabelecidas, documentadas, implementadas, monitoradas e revisadas. | **OpManager Plus:** Utilize o módulo de gerenciamento de configuração para agendar backups de configuração de dispositivos, monitorar atividades de usuários e detectar mudanças comparando versões de configuração a partir de uma interface web centralizada. Garanta a segurança criptografando todos os dados de configuração coletados dos dispositivos com criptografia AES de 256 bits e armazenando-os de forma segura no database.<br><br>**Site24x7:** Utilize a ferramenta de gerenciamento da configuração de rede (NCM) para gerenciar as configurações de dispositivos de rede da sua organização, detectando e corrigindo proativamente configurações incorretas ou alterações não autorizadas. Garanta restauração rápida de configurações funcionais de dispositivos, minimizando interrupções.<br><br>**Endpoint Central:** Proíba a instalação de softwares desnecessários e crie listas de permissão ou bloqueio para o ambiente de TI. Bloqueie a execução automática de executáveis e controle processos filhos originados de outras aplicações. Aplique políticas e configurações de segurança em todos os endpoints e navegadores corporativos. |

| | | |
|---|---|---|
| | | **ServiceDesk Plus:** Crie e mantenha uma CMDB de alta integridade que forneça dados precisos de dependência por meio de mapas visuais. Capture e rastreie dependências com mapeamento de relacionamento integrado a soluções de observabilidade como o Site24x7.<br><br>**Log360:** Monitore e audite alterações de configuração em databases, serviços baseados em cloud e dispositivos de rede para garantir que as configurações de segurança sejam devidamente implementadas e mantidas. |
| 8.10 Exclusão de informações | As informações armazenadas em sistemas de informação, dispositivos ou em qualquer outra mídia de armazenamento devem ser excluídas quando não forem mais necessárias. | **Endpoint Central:** Execute limpezas remotas para garantir a segurança dos dados corporativos em caso de perda de dispositivo.<br>Aplique a compartimentalização em dispositivos móveis para apagar com segurança apenas os dados corporativos, preservando os dados pessoais do usuário. |
| 8.12 Prevenção de vazamento de dados | Devem ser aplicadas medidas de prevenção contra vazamento de dados em sistemas, redes e quaisquer outros dispositivos que processem, armazenem ou transmitam informações sensíveis. | **Endpoint Central:** Utilize recursos avançados de prevenção contra vazamento de dados (DLP) para detectar e classificar informações pessoalmente identificáveis (PII). Tenha controle total sobre o fluxo de dados dentro do ambiente de TI e configure políticas para transferências de dados por meio de serviços baseados em cloud e dispositivos periféricos.<br>Implemente e aplique políticas de BYOD em todos os dispositivos de usuários finais para garantir uma separação clara entre dados pessoais |

| | | |
|---|---|---|
| | | e corporativos, mantendo privacidade e segurança.<br><br>**Log360:** Garanta que as informações sensíveis permaneçam protegidas por meio da detecção e análise em tempo real de movimentações de dados e incidentes de segurança. |
| 8.13<br>Backup de informações | Cópias de segurança de informações, softwares e sistemas devem ser mantidas e testadas regularmente, de acordo com a política específica de backup acordada. | **Log360:** Garanta backups periódicos e integridade dos dados monitorando atividades de backup e restauração, auditando operações de armazenamento e rastreando eventos de sistema. Verifique os processos de backup em database, ambientes baseados em cloud e dispositivos de rede para assegurar conformidade com as políticas e prevenir perda de dados.<br><br>**AD360:** Realize backups periódicos de dados e armazene-os com segurança em múltiplas versões criptografadas, garantindo fácil restauração em caso de perda de dados.<br><br>**PAM360:** Gere backups periódicos de todas as credenciais de identidade privilegiadas, como senhas, chaves SSH, tokens e certificados TLS, em um arquivo ZIP criptografado. Utilize exportações criptografadas de emergência para manter uma cópia de todas as credenciais privilegiadas em fitas de backup ou armazenamento em cloud. |

| | | |
|---|---|---|
| | | **Endpoint Central:** Gere backups instantâneos e não apagáveis dos arquivos da rede a cada três horas utilizando o serviço de cópias de sombra de volume da Microsoft (VSS). Restaure qualquer arquivo infectado por ransomware ou corrompido com sua cópia mais recente de backup com apenas um clique. |
| 8.15<br>Geração de logs | Os logs que registram atividades, exceções, falhas e outros eventos relevantes devem ser gerados, armazenados, protegidos e analisados. | **Log360:** Armazene e proteja logs que capturam atividades, exceções e falhas em todos os sistemas, databases e dispositivos de rede.<br><br>**Endpoint Central:** Audite e rastreie o acesso de usuários a endpoints críticos que executam aplicações sensíveis com relatórios de login detalhados. Gere relatórios de auditoria com informações sobre solicitações de acesso a aplicações bloqueadas.<br><br>**PAM360:** Registre todas as atividades relacionadas ao acesso privilegiado, incluindo solicitações de acesso, aprovações, motivos do acesso e ações executadas nos endpoints acessados.<br><br>**Firewall Analyzer:** Obtenha informações essenciais sobre tentativas de violar a segurança da rede e sobre ataques como trojans, DDoS e outros, por meio de análise detalhada dos logs de segurança do firewall. Utilize relatórios avançados desses logs para realizar análises de segurança, visualizar cenários de ameaças e planejar estratégias de defesa contra tais ataques. |

| | | |
|---|---|---|
| 8.16 Monitoramento de atividades | As redes, sistemas e aplicações devem ser monitorados para detectar comportamentos anômalos, e ações apropriadas devem ser tomadas para avaliar possíveis incidentes de segurança da informação. | **Log360:** Monitore sistemas, redes e aplicações para identificar comportamentos anômalos por meio da análise de atividades de login, eventos do sistema e alterações de configuração.<br><br>**Endpoint Central:** Aproveite o mecanismo integrado NGAV que utiliza tecnologia de aprendizado profundo e detecção comportamental em tempo real assistida por IA para detectar proativamente comportamentos anômalos.<br><br>**PAM360:** Monitore continuamente sessões remotas em tempo real para rastrear atividades de usuários, detectar comportamentos suspeitos e garantir conformidade.<br>Aproveite a integração do PAM360 com o mecanismo UEBA do Log360 para analisar padrões, identificar anomalias e acionar alertas sobre possíveis ameaças de segurança, fortalecendo o controle de acesso e a mitigação de riscos.<br><br>**NetFlow Analyzer:** Utilize o mecanismo de mineração de fluxo contínuo para detectar uma ampla variedade de ameaças de segurança internas e externas. Monitore anomalias de rede que possam contornar o firewall e identifique intrusões de zero-day e comportamentos contextuais suspeitos com precisão.<br><br>**Site24x7:** Monitore redes, sistemas e aplicações para detectar comportamentos anômalos, identificar possíveis incidentes |

| | | |
|---|---|---|
| | | de segurança e acionar respostas adequadas em tempo real. Utilize insights baseados em IA e análise automatizada de causa raiz para garantir mitigação proativa de ameaças e desempenho contínuo da TI.<br><br>**AD360:** Identifique e analise riscos de segurança em ambientes AD e Microsoft 365, incluindo falhas de login, acessos a arquivos, alterações de funções e atualizações de licenças, com o relatório de risco de identidade. O mecanismo UBA integrado ajuda a detectar ameaças internas rastreando usuários mal-intencionados, identificando contas comprometidas e detectando abuso de privilégios. |
| 8.18<br>Uso de programas utilitários privilegiados | O uso de programas utilitários capazes de substituir controles de sistemas e aplicações deve ser restrito e rigidamente controlado. | **ServiceDesk Plus:** Faça a varredura e identifique os softwares instalados nas estações de trabalho, classificando-os como gerenciados ou proibidos. Alerte os responsáveis designados quando um software proibido for identificado. Crie um dashboard de conformidade para identificar violações de políticas de software, como o uso de programas sem licença. |
| 8.19<br>Instalação de software em sistemas operacionais | Devem ser implementados procedimentos e medidas para gerenciar de forma segura a instalação de softwares em sistemas operacionais. | **Endpoint Central:** Implemente softwares com segurança nos sistemas dos usuários finais. Adicione pacotes de software ao portal de autoatendimento dos usuários, permitindo que instalem as aplicações conforme sua conveniência. Proíba a instalação de softwares desnecessários e crie listas de permissão ou bloqueio para o ambiente de TI. |

| | | |
|---|---|---|
| 8.20 Segurança das redes | As redes e os dispositivos de rede devem ser protegidos, gerenciados e controlados para garantir a segurança das informações em sistemas e aplicações. | **OpManager Plus:** Proteja a infraestrutura de rede utilizando protocolos SSH e métodos avançados de autenticação, incluindo autenticação de dois fatores e integração com o AD.<br>**Network Configuration Manager:** Proteja-se contra vulnerabilidades de firmware e simplifique a atualização de firmwares com o uso de configlets.<br><br>**Firewall Analyzer:** Reforce os controles de firewall para fortalecer a segurança da rede de TI. Garanta conformidade com padrões regulatórios do setor. Monitore e analise a atividade de rede para detectar e tratar eventos de segurança anômalos de forma eficaz.<br><br>**Log360:** Proteja e gerencie dispositivos de rede monitorando atividades de login, alterações de configuração e eventos de segurança.<br><br>**Endpoint Central:** Configure o firewall do Windows para os usuários finais. Realize auditorias detalhadas de portas no ambiente de TI e reduza a superfície de ataque bloqueando e protegendo portas abertas. Garanta navegação segura aplicando configurações avançadas de proteção contra ameaças. Impeça que os usuários baixem arquivos potencialmente maliciosos ou acessem sites conhecidos por conter ameaças. Reforce a segurança dos servidores web e corrija configurações incorretas.<br><br>**AD360 ou Identity360:** Proteja o acesso a todos os endpoints das redes corporativas com métodos sólidos de MFA. |

| | | |
|---|---|---|
| 8.21 Segurança dos serviços de rede | Os mecanismos de segurança, níveis de serviço e requisitos dos serviços de rede devem ser identificados, implementados e monitorados. | **Firewall Analyzer:** Monitore e gere relatórios sobre o uso de regras, políticas e listas de controle de acesso (ACLs) do firewall. A ferramenta coleta todas as regras do firewall e gera relatórios detalhados de uso por regra, permitindo avaliar a eficácia das regras e otimizá-las para melhorar o desempenho e a segurança. |
| 8.22 Segregação de redes | Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados nas redes da organização. | **Endpoint Central:** Utilize o recurso de grupos personalizados para segregar logicamente os sistemas e gerenciá-los de forma mais eficiente e segura. Crie diferentes grupos estáticos ou dinâmicos para diferentes ambientes operacionais conforme as necessidades da organização. |
| 8.23 Filtragem da web | O acesso a sites externos deve ser gerenciado para reduzir a exposição a conteúdos maliciosos. | **Endpoint Central:** Bloqueie sites maliciosos para impedir que os usuários acessem conteúdo potencialmente prejudicial. |
| 8.24 Uso de criptografia | Devem ser definidas e implementadas regras para o uso eficaz de criptografia, incluindo o gerenciamento de chaves criptográficas. | **Endpoint Central:** Criptografe dispositivos de usuários finais utilizando o BitLocker para sistemas Windows e o FileVault para dispositivos Mac.<br><br>**PAM360:** Criptografe todas as informações pessoais identificáveis (PII), credenciais sensíveis, contas e outras entidades críticas tanto no nível da aplicação quanto no database, utilizando o algoritmo de criptografia simétrica AES-256. Armazene apenas os dados criptografados no database de senhas. |

| | | |
|---|---|---|
| 8.32 Gerenciamento de mudanças | As mudanças em instalações de processamento da informação e sistemas de informação devem estar sujeitas a procedimentos de gerenciamento de mudanças. | **ServiceDesk Plus:** Gerencie alterações em instalações e sistemas de processamento da informação com recursos de gerenciamento de mudanças certificados pelo ITIL. Gerencie mudanças por meio de workflows definidos, mecanismos de avaliação de riscos com IA e procedimentos de autorização para minimizar riscos e violações de conformidade.<br><br>**OpManager Plus:** Gerencie mudanças de forma eficaz utilizando o módulo de gerenciamento de configuração. Receba notificações em tempo real sobre alterações, impeça modificações não autorizadas com controle de acesso baseado em função (RBAC), reverta rapidamente para versões confiáveis com a funcionalidade de rollback e identifique facilmente diferenças de configuração com o recurso Diff View, que oferece comparações codificadas por cores dentro do produto. |

# Produtos da ManageEngine e controles ISO 27001 correspondentes

| Produtos da ManageEngine | Controles compatíveis |
|---|---|
| ServiceDesk Plus | 5.9, 5.11, 5.15, 5.18, 5.19, 5.21, 5.23, 5.24, 5.25, 5.26, 5.27, 5.28, 5.31, 5.34, 5.36, 6.8, 7.10, 7.14, 8.1, 8.9, 8.18, 8.32 |
| Endpoint Central | 5.7, 5.9, 5.11, 5.12, 5.13, 5.15, 5.17, 5.18, 5.28, 5.30, 5.31, 5.32, 5.33, 5.34, 5.36, 6.7, 7.10, 7.14, 8.1, 8.2, 8.3, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 8.12, 8.13, 8.15, 8.16, 8.19, 8.20, 8.22, 8.23, 8.24 |
| AD360 | 5.15, 5.16, 5.17, 5.18, 5.33, 5.34, 5.36, 6.7, 8.1, 8.3, 8.5, 8.7, 8.13, 8.16, 8.20 |
| Identity360 | 5.15, 5.16, 5.18, 5.34, 8.1, 8.3, 8.5, 8.20 |
| PAM360 | 5.9, 5.11, 5.15, 5.18, 5.28, 5.33, 6.7, 8.2, 8.3, 8.5, 8.13, 8.15, 8.16, 8.24 |
| Log360 | 5.7, 5.9, 5.11, 5.14, 5.15, 5.17, 5.18, 5.23, 5.26, 5.28, 5.31, 8.7, 8.9, 8.12, 8.13, 8.15, 8.16, 8.20 |
| OpManager Plus | 5.9, 5.15, 5.18, 5.31, 5.34, 5.36, 8.5, 8.6, 8.8, 8.9, 8.20, 8.32 |
| Site24x7 | 5.9, 5.23, 8.6, 8.9, 8.16 |
| Analytics Plus | 5.9, 5.11, 5.32, 6.7, 8.6 |
| AppCreator | 5.9, 5.11, 5.15, 5.18, 5.34 |
| Firewall Analyzer | 5.36, 8.15, 8.20, 8.21 |
| DataSecurity Plus | 5.9, 5.11, 5.12 |
| AssetExplorer | 5.9, 5.11 |
| Network Configuration Manager | 8.20 |
| NetFlow Analyzer | 8.16 |

# Assuma o controle da sua TI

## Gerencie, monitore e proteja sua empresa digital com a ManageEngine.

### Gerencie identidades e acessos digitais

Administre, governe e proteja identidades digitais em toda a organização com orquestração de identidade, segurança de acesso privilegiado, CIEM, MFA, SSO e controles de acesso baseados em função, e muito mais.

manageengine.com/iam

### Ofereça experiências de serviço inteligentes

Aprimore seus workflows de entrega de serviços com as melhores práticas de ITSM, automação e IA nativa.

manageengine.com/usm

### Controle e proteja todos os endpoints

Gerencie, proteja e controle todos os endpoints em áreas como computação do usuário final, cibersegurança, governança, risco e conformidade, I/O, e muito mais.

manageengine.com/uems

### Fortaleça operações de rede e TI

Alcance visibilidade total sobre sua rede e stack de aplicações com observabilidade orientada por IA. Resolva problemas proativamente, otimize o desempenho e fortaleça a segurança.

manageengine.com/itom

### Reforce a segurança e conformidade de TI

Detecte, investigue e responda a ameaças com UEBA, inteligência de ameaças e monitoramento de logs. Garanta conformidade e mitigue riscos com relatórios prontos para auditoria.

manageengine.com/siem

### Insights unificados de toda a TI

Visualize cada aspecto da TI e identifique riscos com antecedência, obtendo estratégias contextuais práticas para eliminar gargalos operacionais.

manageengine.com/ita

### Otimize a TI com aplicações low-code

Amplie as capacidades dos seus processos de TI combinando low-code e GenAI. Resolva desafios rapidamente e inove com o mínimo de programação.

manageengine.com/lowcode

# Sobre a ManageEngine

A ManageEngine produz o maior conjunto de software de gerenciamento de TI do setor, com mais de 60 produtos para administrar todas as operações de TI — desde redes e servidores até aplicações, service desk, Active Directory, segurança, desktops e dispositivos móveis.

Desde 2002, equipes de TI em todo o mundo confiam em nossas soluções acessíveis, completas e fáceis de usar.

À medida que sua organização se prepara para os desafios futuros, continuaremos liderando com novas soluções, integrações contextuais e inovações que só uma empresa totalmente dedicada a seus clientes pode oferecer. Como uma divisão da Zoho Corporation, continuamos impulsionando a convergência entre negócios e TI, ajudando você a aproveitar as oportunidades do futuro.

ManageEngine

uma divisão da **Zoho** Corp.

Para saber mais, acesse

**www.manageengine.com | sales@manageengine.com**