|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [Traduzido do Inglês para o Português - www.onlinedoctranslator.com](https://www.onlinedoctranslator.com/pt/?utm_source=onlinedoctranslator&utm_medium=docx&utm_campaign=attribution)  1. Em geral  1.1 Propósito  1.2 Alcance  1.3 Estabelecimento, revisão/revogação e emissão  1.4 Definições  2. Garantindo a segurança do produto    3. Operações de segurança do produto  3.1 Estipulação de regras operacionais e promoção de operações  3.2 Determinação de produtosprecisandomedidas de segurança  3.3 Gerenciamento de riscos  3.4 Operações de segurança do produto no desenvolvimento, manutenção e outros processos  3,5 Medidas de segurança da informação para o ambiente de desenvolvimento  3.6 Controle de configuração  3.7 Controle de vulnerabilidade de componentes adquiridos que constituem produtos  3.8 ºreata análiseeavaliação de risco  3.9 Determinação dos requisitos de segurança  3.10 Projeto de segurança do produto e implementação    3.11 Confirmação da implementação do projeto de segurança do produto  3.12 Planejamento e implementação de verificação de vulnerabilidade  3.13 Desenvolvimento de diretrizes  3.14 Atividades de manutenção da qualidade da segurança do produto  3.15 Entregando aos processos de pós-desenvolvimento  3.16 Gerenciamento deterceirizared organizações externas  3.17 Melhoria continua  4. Ação contra incidentes de segurança do produto  5. Inspeção e melhoria das operações  6. Controle de documentos/registros  Disposições suplementares | O objetivo dessas Normas é fornecer produtos seguros e confiáveis, garantindo a segurança dos produtos de acordo com as“Regras de operação de segurança do produto” (APQ-AS-001) deos Eletrodomésticos e Soluções VivasCompanhiada Panasonic Corporation (doravante referida como “LAS").  Estas Normas aplicam-se a produtos e sistemas que sãoprojetado, produzido,distribuídos ou atendidos porLAS edivisões (incluindo empresas estrangeiras) às quais os padrões de qualidade da LAS são aplicados (incluindouding serviços, ferramentas de suporte, bibliotecas, etc. por meio decomputadoraplicativos, aplicativos de smartphone ou aplicativos da web; com ou sem taxas). As Normas também se aplicam a ddesenvolvimento para alterações pós-envio [upgrades de versão].  Estas Normas serão estabelecidas, revisadas e revogadas pelo Diretor doLASQualidadeInovaçãoCentro, e emitido pelo Gerente Geralencarregado de sfrequentementequality.  Para os fins destas Normas, os seguintes termos terão os significados definidos nos respectivos itens, exceto que as definições de outros termos utilizados nestas Normas deverão estar de acordo com as Regras Operacionais de Segurança do Produto.  (1) Operações relacionadas à segurança do produto: Todas as operações relacionadas à garantia da segurança do produto ao longo de todo o ciclo de vida dos produtos, incluindo planejamento, projeto, desenvolvimento, manutenção, etc., necessárias para fornecer produtos seguros e confiáveis ​​usando tecnologia da informação (TI)  (2) Produtos que usam TI (doravante denominados "Produtos de TI"): Equipamentos que usam redes e outras TI, e todos os negócios de serviços que acompanham oequipamento.  (3) Vulnerabilidade: Problemas nas especificações de Produtos de TI que podem ser explorados por terceiros para um ato que represente uma ameaça (tomada de controle de um sistema, vazamento de informações confidenciais etc.)  (4) Vulnerabilidade conhecida: Vulnerabilidade cuja existência foi reconhecida e cujas informações foram fornecidas  (5) Pesquisa de vulnerabilidade: para verificar se existe ou não vulnerabilidade no software e em outros componentes, reunindo informações públicas e informações de fornecedores de componentes.  (6) Incidentes de segurança do produto: vulnerabilidade que pode resultar na execução de um ataque maliciosonotificado à empresa(tanto divulgado como não divulgado) e ocorrência real de um ataque malicioso  (7) Riscos: Impacto da incerteza em um propósito. Para os propósitos destes Padrões, "riscos" significa aqueles associados à segurança do produto.  (8) Riscos residuais: riscos que permanecem após algumas ações terem sido tomadas contra os riscos originais e ainda podem afetar os clientes ou nossos negócios  (9) Requisitos de segurança: Requisitos que definem as funções que os produtos devem ter em relação aos requisitos do cliente, dadas as características dos riscos associados aos produtos  (10) Componentes adquiridos: Componentes fabricados oupossuídopor outras empresas ("Componentes" incluem hardware e software.) que foram adquiridos por meio de compra ou outros meios legais (os componentes cuja produção é terceirizada devem ser gerenciados como parte do processo de terceirização e excluídos dos componentes adquiridos aqui definidos.)  (11) Conexão: Cconexão entre o produto e dispositivos externos    Para garantir a segurança dos Produtos de TI, todos os processos ao longo de todo o ciclo de vida doTI Pos produtos devem ser esclarecidos e a correlação entre os processos e as operações relacionadas à segurança do produto deve ser identificada e gerenciada.  Operações e procedimentos específicos devem ser implementadoscom referência aas "Regras Operacionais para Segurança do Produto" e "Padrões Operacionais para Segurança do Produto", bem como as diretrizes relevantes, incluindo "Segurança do Produto - Diretrizes de Análise de Ameaças", "Segurança do Produto - Diretrizes de Design", Panasonic "Diretrizes do Processo de Desenvolvimento de Software", eLAS“Diretrizes de Resposta a Incidentes de Segurança do Produto” (APQ-MQ-003).  Abaixo estão descritas as principais operações a serem realizadas para garantir a segurança do produto.  As divisões devem estipular as regras operacionais internas de segurança do produto de acordo com as regras e padrões da LAS e promover as operações de acordo.  O Departamento de Design/Desenvolvimento deve assumir a liderança para determinar se um Produto de TI precisa de medidas de segurança na fase de análise de requisitos de software\* (conforme indicado na Panasonic “Diretrizes do Processo de Desenvolvimento de Software”) e descrever os resultados em uma Planilha de Política de Planejamento (Anexo 1, “Padrões de Operação de Planejamento de Produto” [APQ-BD-001]).Smedidas de segurança devem ser tomadas paraTI Pprodutos que se enquadrem em qualquer um dos seguintes critérios.Produtos de TI para os quais as medidas de segurança são exigidas por leis/regulamentos eindustrialas regras e normas também devem ser tratadas como produtos que necessitam de medidas de segurança.  [Critério]   |  | | --- | | ① Equipado com funções de criptografia, autenticação ou PKI (Public Key Infrastructure) | | ② Equipado com funções para armazenar/utilizar informações pessoais dos usuários | | ③ Equipado com funções que usam informações biométricas | | ④ Equipado com funções para gerenciar/proteger os ativos dos usuários (informações pré-pagas, dinheiro eletrônico, informações de crédito, chaves, etc.) | | ⑤ Equipado com funções para proteger direitos autorais | | ⑥ Equipado com uma interface para conexão com produtos de TI\*  (HDMI, USB, LAN com fio/sem fio, Wi-Fi, BT, NFC, SD, etc. Produtos de TI que usam LAN com fio/sem fio como interface são considerados como tendo funções de conexão de rede, como Internet e Intranet.) | | ⑦ Equipado com funções que permitem aos usuários alterar programas ou funções que permitem fazê-lo usando programas baixados |   \* Se um protocolo não divulgado externamente exclusivo de um Produto de TI for usado para comunicação entre partes de um único Produto de TI, as medidas de segurança do produto não serão necessárias para esses produtos, pois a proteção é fornecida no Produto de TI.  As Divisões devem coletar continuamente informações sobre os produtos pelos quais são responsáveis ​​e, quando julgar necessário, gerenciar os riscos relevantes, analisando-os e avaliando-os. Os tipos de informações sobre riscos que precisam ser coletados continuamente incluem informações sobre leis/regulamentos e regras e padrões industriais, e informações contingentes a mudanças no usomeio Ambiente, bem como informações sobre novas ameaças e vulnerabilidades.  Caso seja difícil tomar medidas contra os riscos imediatamente ou qualquer risco permaneça após as devidas ações terem sido tomadas, as divisões relevantes devem gerenciar esses riscos como riscos residuais após consultar a pessoa responsável pela implementação das operações de segurança do produto.  As divisões devem preparar padrões operacionais para segurança do produto para seu desenvolvimento, manutenção e outros processos. As entregas de cada processo devem ser preparadas e verificadas de acordo com os padrões relevantes.  As divisões devem manter a segurança da informação para o ambiente de desenvolvimento de acordo com as regras estipuladas por seusem formaçãodepartamento de sistema.  As divisões devem, como parte de seu controle de configuração das entregas de cada processo, controlar as entregas relacionadas à segurança do produto, a fim de manter a consistência e a integridade das entregas dos produtos que precisam de medidas de segurança e implementar detalhes de projeto corretos nos produtos (exemplo de caso de controle: controlando as entregas mantendo as versões e linhas de base das entregas atualizadas).  As divisões devem controlar a vulnerabilidade conhecida dos componentes adquiridos ao longo de todo o ciclo de vida do produto, a fim de evitar a ocorrência de problemas devido à vulnerabilidade dos componentes adquiridos que constituem produtos. Os componentes adquiridos que são usados ​​devem ser registrados com um sistema de controle de vulnerabilidades pelo AQ2, de modo a gerenciar continuamente as informações sobre vulnerabilidade que podem ser relatadas após o envio e tomar as medidas apropriadas quando necessário (exemplo de caso de controle: Realização de pesquisa sobre vulnerabilidade conhecida no momento de aceitar componentes adquiridos, tomando ações com base em descobertas de vulnerabilidadeem formaçãorecolhidos após o envio, etc.)  As divisões devem analisar as ameaças esperadas dos produtos que precisam de medidas de segurança e discutir as medidas de proteção que podem ser necessárias para a avaliação de risco, a fim de determinar os requisitos de segurança do produto e gerenciar os riscos residuais.  Ao analisar ameaças e avaliar riscos, técnicas/procedimentos padrão devem ser adotados. TeleO Gerente de Operações de Segurança do Produto deve solicitar que os departamentos relevantes realizem análises de ameaças. Em princípio, a análise de ameaças deve ser conduzida pela AQ0 e as medidas necessárias também devem ser concluídas. A análise de ameaças também deve ser conduzida quando ocorrer uma mudança de projeto.  Se não houver alterações na função para garantir a segurança do produto em relação ao modelo anterior e a natureza da ameaça permanecer inalterada, os resultados da análise do modelo anterior poderão ser usados ​​para análise de ameaças do modelo atual, desde que sejam fornecidas suas razões . No entanto, quando os resultados da análise do modelo anterior forem utilizados por três anos ou mais, uma revisão deve ser realizada levando em consideraçãocontamudanças no ambiente e técnicas de ataque. Tais mudanças no ambiente incluem mudanças nas leis/regulamentos, regras e padrões industriais e no ambiente de uso, bem como informações sobre novas ameaças e vulnerabilidades.  As divisões determinarão a segurançarequisitoscom base nos resultados da análise de ameaças, etc., conforme estipulado em 3.8 deste documento e levando em consideração os riscos associados às funções do produto e fatores externos.  As divisões devem conduzir o projeto com base nas melhores práticas de projeto de segurança, como as "Diretrizes de Projeto de Segurança do Produto (TM156)", a fim de implementar todos os requisitos de segurança do produto determinados em 3.9, conforme pretendido.  Ao implementar o software, as regras que consideram a segurança devem ser estabelecidas na forma de regras de codificação, etc., de acordo com as quais a codificação deve ser conduzida.  As divisões devem realizar análises estáticas, revisões e testes de confirmação de implementação para garantir que os requisitos de segurança do produto tenham sido adequadamenteimplementadonos produtos que eles têmdesenvolvido.  O Departamento de Design/Desenvolvimento deve, durante o ciclo de vida do produto, planejar a verificação de vulnerabilidade e solicitar ao Centro de Segurança do Produto ou outros órgãos de verificação que realizem verificação especializada para TIProdutos.Sediadasobre os resultados da verificação de vulnerabilidades, as vulnerabilidades com alto risco (NG3) devem ser eliminadas pelo AQ1. Se, por algum motivo, tais riscos não puderem ser eliminados e permanecerem, ações separadas devem ser discutidas.  <Critérios para verificação de vulnerabilidades (Resultados da verificação especializada pelo Product Security Center)>   |  |  | | --- | --- | | NG3 (alto risco) | - Pode resultar diretamente em vazamento de informações, falsificação, falha/reinicialização, tomada de controle, infecção por malware e falsificação(confidencialidade/integridade/disponibilidade) | | NG2 (risco médio) | - Não resultar diretamente em vazamento de informações  - Para que ataques sejam feitos, são necessárias condições limitadas (acesso a uma página de trap, etc.) | | NG1 (baixo risco) | - Não resultar diretamente em vazamento de informações  - Para que os ataques sejam feitos, são necessárias condições mais rigorosas do que as do NG2 acima | | PD (fornecimento de informações) | - Não causa risco por si só  - Pode fornecer uma dica para localizar outras vulnerabilidades |   As divisões devem desenvolver diretrizes para garantir que os usuários usem os produtos que precisam de segurança do produto de forma adequada e segura. Para os propósitos destes Padrões, as diretrizes referem-se a todas as medidas com as quais chamar a atenção dos usuários, incluindo, mas não se limitando a, instruções de áudio, visual e vídeo, bem como instruções de operação, guias de instalação e outros documentos.  As cinco atividades a seguir devem ser conduzidas para manter a qualidade da segurança do produto de novos produtos ao longo do processo de desenvolvimento, garantindo assim a qualidade da segurança do produto no momento do embarque e durante todo o ciclo de vida do produto.  “Atividades de manutenção da qualidade” aqui se refere às “atividades de manutenção da qualidade” no Anexo 2.   1. Verificação da seleção de produtos de TI que precisam de medidas de segurança com base nos critérios (pela Política de Planejamento, em princípio)   - Confirmar que os produtos são selecionados adequadamente de acordo com os critérios   1. Verificação dos resultados da análise de ameaças(por AQ0, em princípio)   - Confirme se a análise de ameaças foi concluída,em formaçãoativos foram determinados, os riscos foram avaliados com base em ativos e ameaças e a necessidade de agir contra ameaças (verificação de documentos)   1. Verificação deevidência de que ações de design foram tomadas contra ameaças   - Confirme os resultados da verificação do conteúdo das alterações de projeto e ações tomadas posteriormente e seu impacto   1. Verificardovulnerabilidadeverificaçãoresultados (por AQ1)   - Confirme se as ações foram tomadas contra os problemas assim identificados  (Ações contra NG3, em particular)   1. Monitoramento de eventos de segurança do produto ao longo do ciclo de vida do produto   - As informações de segurança sobre os produtos após o envio devem ser coletadas por cada departamento relevante. Caso a vulnerabilidade seja relatada, as ações necessárias e os esforços de melhoria devem ser feitos de acordo com o LAS "Diretriz de resposta a incidentes de segurança do produto" (APQ-MQ-003), mantendo assim a qualidade da segurança do produto.  Abaixo estão os principais papéis e perspectivas dos departamentos envolvidos em cada tarefa, incluindo as atividades de manutenção da qualidade①～⑤acima de. (O seguinte "Não". indica as atividades de manutenção de qualidade correspondentes acima.)   |  |  |  | | --- | --- | --- | | Tarefas | Não. | Departamentos | | Seleção de produtos de TI que precisam de medidas de segurança | ① | Desenvolvimento de elementos, design/desenvolvimento | | Tanálise de ameaças, design de segurança do produto, codificação segura,análise estática / revisão e testes confirmatórios de implementação, verificação de vulnerabilidade, registro de software em uso com o sistema de gerenciamento de vulnerabilidade |  | Desenvolvimento de elementos, design/desenvolvimento | | Confirmação de que as atividades para melhorar a qualidade da segurança do produto são realizadas no processo de desenvolvimento e que a prevenção de recorrência é realizada  Confirmação do design de segurança e os resultados da verificação de vulnerabilidade |  | Qualidade, SQA | | Confirmação deevidência dequalidade de segurança do produto com base em documentos de decisão de embarque enviados para estudo de protótipo de produção em massa  - Tque a análise de ameaças foi concluída e as políticas para riscos residuais foram anunciadas e aprovadas  - Essa verificação de vulnerabilidade foi concluída  - Essa vulnerabilidade de alto risco (NG3) está ausente ou já foi tratada | ②  ③  ④ | *Shinsa*(avaliação) | | Confirmação dos resultados da análise de ameaças, design de segurança e resultados da verificação de vulnerabilidades | ②③④ | Departamento responsável por sfrequentementeqrealidade, QualidadeInovaçãoCentro | | Monitoramento de informações de vulnerabilidade após o envio e tomada de açãoquando ocorre um incidente | ⑤ | Design/desenvolvimento, qualidade, SQA, Departamento responsável pela qualidade de software, Centro de Inovação em Qualidade | | Monitoramento e correção das medidas de segurança do produto |  | Qualidade,SQA |   As divisões devem, de acordo com as regras do departamento de sistema de informação, departamento de produção e outros departamentos relevantes, tomar medidas de segurança apropriadas nos pontos de produção, armazenamento edistribuiçãoapós o produto ter sido desenvolvido.  As divisões devem, quando terceirizam seu desenvolvimento, manutenção ou outras operações relacionadas a produtos que necessitem de medidas de segurança de produtos, gerenciar organizações externas terceirizadas relevantes, a fim de realizar operações de segurança de produtos em conformidade com suas regras divisionais (exemplo de itens de controle: seleção de organizações externas terceirizadas , requisitos no momento da assinatura do contrato, ferramentas utilizadas e o que aceitar de organizações externas terceirizadas).  Quando a verificação de vulnerabilidade encontrar um problema que precise ser melhorado, etc., medidas para mitigar ameaças potenciais devem ser refletidas no projeto para que tais riscos possam ser reduzidos continuamente em produtos futuros.  Os departamentos relevantes devem, após o recebimento deem formaçãosobre incidentes de segurança do produto, comunique imediatamente essa informação ao responsável pela promoção do produtosegurança, o Gerente Geral de Segurança do Produto do produto relevante e o escritório LAS-IRT de acordo com o LAS "Diretriz de resposta a incidentes de segurança do produto" (APQ-MQ-003)  As divisões devem estipular regras de auditoria e autoverificação para garantir que as medidas de segurança do produto sejam tomadas de forma adequada, promovendo assim a melhoria das operações.  Os registros relacionados a estes Padrões de Operação devem ser mantidos sob controle de acordo com os “Padrões de Controle de Documentos de Qualidade e Registros de Qualidade” (APQ-BG-001).  Estas Normas entrarão em vigor em 1º de abril de 2022. | 2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2 |