

25 de agosto de 2015

Requisitos de Segurança da Informação para Fornecedores da Johnson & Johnson

Este documento especifica os requisitos de segurança da informação aplicáveis aos Fornecedores que proveem mercadorias ou serviços para a Johnson & Johnson e/ou para Afiliada Johnson & Johnson, sendo tais requisitos baseados na International Organization for Standardization (ISO) 27001. As classificações de dados da Johnson & Johnson estão totalmente definidas na seção “Definições” abaixo. O Fornecedor é responsável por compreender a classificação da informação da Johnson & Johnson e da Afiliada Johnson & Johnson que irá acessar, processar, ou armazenar na execução do serviço à Johnson & Johnson ou à Afiliada Johnson & Johnson.

Os “Requisitos de Somente Acesso à Internet” significam os requisitos aplicáveis estabelecidos apenas nas seguintes seções destes Requisitos de Segurança da Informação para Fornecedores: 1.1, 1.2.1, 1.2.4, 1.3.4, 1.4, 1.6.7-1.6.13 relativos a Sistemas de Usuário, 1.6.26, 1.7.1-1.7.21, 1.7.28-1.7.39 relativos a Sistemas de Usuário, 1.7.40-1.7.42, 1.8.16-1.8.18 relativo a Sistemas de Usuário, e 1.11.

DEFINIÇÕES

As definições a seguir contêm uma série de termos que são utilizados ao longo deste documento. Ao encontrar algum dos termos destacados, refira-se à definição abaixo.

Afiliada Johnson & Johnson: Qualquer entidade que controla, que é controlada por, ou que está sob controle comum da Johnson & Johnson.

Aplicações dentro do Escopo: Aplicações, incluindo bancos de dados e websites voltados à Internet que armazenam, transmitem, ou processam Informação Classificada da Johnson & Johnson, ou websites voltados à Internet que contêm informação pública da Johnson & Johnson.

Dispositivos Computacionais Móveis: Dispositivo computacional pessoal de mão capaz de armazenar informações e de comunicar-se a partir de redes sem fio (incluindo celular e/ou Wi-Fi), tais como, smartphones, tablets e PDAs.

Dispositivos de Rede: Sistemas e ferramentas que sejam parte da infraestrutura de rede, tais como, roteadores, switches, firewalls, servidores de cache e de proxy, e balanceadores de carga.

Dispositivos Removíveis de Armazenamento: Qualquer dispositivo portátil ou removível que armazena informação eletrônica e que pode ser facilmente removido e transportado (por exemplo, disco rígido portátil, pen drive, cartão de memória, CD, DVD, fita ou dispositivo de back-up, etc.).

Informação Classificada da Johnson & Johnson: Dados da Johnson & Johnson e de Afiliada Johnson & Johnson, incluindo Informações Pessoais da Johnson & Johnson, os quais, se divulgados a partes não autorizadas, podem resultar em impacto negativo nos lucros da Johnson & Johnson ou de Afiliada Johnson & Johnson. A Informação Classificada da Johnson & Johnson será identificada dessa forma e pode ser designada como “Informação Confidencial” (impacto moderado, se divulgada a partes não autorizadas), “Informação Restrita” (impacto sério, se divulgada a partes não autorizadas), ou “Informação Altamente Restrita” (impacto muito sério, se divulgada a partes não autorizadas, incluindo Informações Pessoais Especiais da Johnson & Johnson). As senhas utilizadas para proteger Informação Classificada da Johnson & Johnson são consideradas Informação Altamente Restrita.

Informação da Johnson & Johnson: Dados da Johnson & Johnson e/ou de Afiliada Johnson & Johnson, que incluem, mas não se limitam a Informação Classificada da Johnson & Johnson, Informação Pessoal da Johnson & Johnson, Informação Pessoal Especial da Johnson & Johnson, ou informação pública da Johnson & Johnson e de Afiliada Johnson & Johnson que é provida ao Fornecedor para armazenamento da informação em um website voltado à Internet hospedado pelo Fornecedor ou aplicação web hospedada pelo Fornecedor.

Informação Pessoal da Johnson & Johnson: Dados da Johnson & Johnson e de Afiliada Johnson & Johnson que identificam ou podem ser utilizadas para identificar um indivíduo.

Informação Pessoal Especial da Johnson & Johnson: Dados da Johnson & Johnson e de Afiliada Johnson & Johnson que incluem qualquer tipo de informação pessoal a seguir: (i) número de Seguro Social, número de identificação de contribuinte, número de passaporte, número de carteira de motorista ou outro número de identificação emitido pelo governo; ou (ii) detalhes de cartão de crédito ou de débito ou número de conta bancária, com ou sem qualquer código ou senha que permita acesso à conta; histórico de crédito, ou (iii) informação sobre raça, religião, etnia, orientação sexual, informação médica ou de saúde, informação genética ou biométrica, crenças políticas ou filosóficas, participação em sindicatos, informação sobre antecedentes, dados judiciais como registros criminais ou informação sobre processos judiciais ou administrativos.

Recursos Computacionais e de Rede: Todos os Sistemas, Aplicações dentro do Escopo, Dispositivos de Rede e serviços de rede.

Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores: Os requisitos descritos neste documento.

Sistemas: Sistemas de Usuários e Sistemas de Servidores.

Sistemas de Servidores: Sistemas computacionais compartilhados, incluindo servidores que fornecem arquivo e impressão, colaboração, grupos de trabalho, mensagem instantânea, transferência de arquivos, aplicações, ou serviços de e-mail.

Sistemas de Usuários: Dispositivo computacional pessoal utilizado por um usuário final, incluindo desktops, laptops, estações de trabalho, e Dispositivos Computacionais Móveis.

1.1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- 1.1.1. O Fornecedor tem de possuir políticas de segurança da informação documentadas e implementadas a fim de assegurar a confidencialidade, integridade e disponibilidade da Informação do Fornecedor e da Johnson & Johnson.
- 1.1.2. O Fornecedor tem de possuir uma política formal e uma prática que suporte à classificação da informação em sua organização.
- 1.1.3. O Fornecedor tem de revisar anualmente suas políticas de segurança da informação a fim de assegurar que as políticas enderecem novas ameaças. A revisão do Fornecedor deverá prever razoavelmente riscos internos ou externos à segurança, confidencialidade, e integridade da Informação da Johnson & Johnson, esteja ela em meio eletrônico, em papel, ou outro tipo de registro e, quando necessário, avaliar e melhorar a eficácia de suas medidas de segurança para limitar os riscos identificados.

1.2. ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

ORGANIZAÇÃO INTERNA

- 1.2.1. O Fornecedor deverá designar um indivíduo responsável pela segurança da informação dentro de sua organização ("Information Security Officer") e definir os papéis e responsabilidades de segurança da informação em toda a organização. O Fornecedor deverá prover o nome e as informações de contato de seu Information Security Officer quando solicitado.

PARTES EXTERNAS

- 1.2.2. O Fornecedor deverá assegurar que haja acordos de confidencialidade vigentes com quaisquer contratados, subcontratados, e outras partes relacionadas que tenham acesso à rede interna do Fornecedor e/ou que armazenem, processem, ou transmitam Informação Classificada da Johnson & Johnson.

- 1.2.3. O Fornecedor deverá conduzir avaliações dos contratados, subcontratados, e outras partes relacionadas conforme os Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores antes de compartilhar Informação Classificada da Johnson & Johnson com eles, ou de estabelecer uma conexão rede-a-rede entre sua rede a rede interna do Fornecedor, ou de hospedar um website ou uma aplicação web contendo Informação da Johnson & Johnson.
- 1.2.4. O Fornecedor deverá ser responsável por assegurar que os requisitos de segurança, incluindo os Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores aplicáveis, estejam contidos nos contratos com, e sejam atendidos por, todos os contratados, subcontratados e outras partes relacionadas do Fornecedor que tenham acesso a, ou que irão armazenar, processar, ou transmitir Informação Classificada da Johnson & Johnson ou que irão hospedar um website contendo Informação da Johnson & Johnson.

1.3. GESTÃO DE ATIVOS

- 1.3.1. O Fornecedor deverá manter um inventário de seus ativos de hardware e software que documente a identificação, propriedade, uso, localização e configuração para cada item.
- 1.3.2. O Fornecedor deverá manter documentação e outros registros de configuração básica de sistemas e de segurança, incluindo mudanças de configuração para todos os componentes de hardware e software dos sistemas.
- 1.3.3. O Fornecedor deverá possuir políticas e práticas formais para elaborar avaliações de risco de software, de sistemas e das instalações. Isso inclui classificar a informação e os sistemas de informação, identificar os requisitos de segurança, avaliar e assegurar a aderência às políticas do Fornecedor e a outros requisitos aplicáveis, e cumprir com o processo de gestão de mudança.
- 1.3.4. O Fornecedor deverá ter controles implementados a fim de assegurar que seus empregados, contratados e outros usuários respeitem o uso aceitável e outras políticas a fim de assegurar a aderência aos Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores, bem como os próprios requisitos do Fornecedor.

1.4. SEGURANÇA DOS RECURSOS HUMANOS

- 1.4.1. O Fornecedor deverá assegurar que seus empregados, contratados e outros usuários compreendam suas responsabilidades com relação à segurança da informação, recebam o treinamento inicial e periódico para reciclagem sobre segurança da informação e assinem os acordos de confidencialidade a fim de assegurar a proteção da Informação da Johnson & Johnson.
- 1.4.2. O Fornecedor deverá conduzir verificação de antecedentes e/ou outras investigações que se façam necessárias, de maneira apropriada e permitida por lei, sobre os indivíduos. O Fornecedor deverá realizar investigações adicionais de acordo com a criticidade da posição e da informação a que o indivíduo pode ter acesso, conforme permitido por lei.
- 1.4.3. O Fornecedor deverá assegurar que seus administradores sejam adequadamente treinados sobre os Recursos Computacionais e de Rede dos quais são responsáveis, e que os registros de treinamento sejam mantidos.
- 1.4.4. O Fornecedor deverá possuir um processo implementado de medidas para os casos de violação de políticas.
- 1.4.5. O Fornecedor deverá remover imediatamente o acesso de usuário aos Recursos Computacionais e de Rede do Fornecedor e às instalações e às áreas seguras (por

exemplo, data centers, cabines de telecomunicações, etc.) quando um indivíduo deixa de trabalhar para o Fornecedor, ou quando não mais necessita do acesso.

1.5. SEGURANÇA FÍSICA E DO AMBIENTE

ÁREAS SEGURAS

- 1.5.1. O Fornecedor deverá implementar mecanismos de controle de acesso físico (por exemplo, controle eletrônico de acesso, fechaduras) a fim de assegurar que apenas os indivíduos autorizados possam obter acesso físico às instalações do Fornecedor.
- 1.5.2. O Fornecedor deverá trancar e/ou possuir controles de acesso robustos implementados a fim de controlar o acesso a todos os seus data centers, salas de equipamentos, cabines de telecomunicação e de serviços.
- 1.5.3. O Fornecedor deverá controlar o acesso não autorizado às áreas não vigiadas (por exemplo, escritórios, salas de conferência, etc.) utilizando fechaduras ou meios equivalentes dentro das instalações de um Fornecedor que contenham Informação Classificada da Johnson & Johnson.
- 1.5.4. O Fornecedor deverá conduzir inspeções de perímetro e de todos os mecanismos de controle de controle a cada dois anos a fim de assegurar que seu hardware não possa ser facilmente manipulado ou violado para obter-se acesso não autorizado.
- 1.5.5. O Fornecedor deverá assegurar que suas instalações e data centers estão protegidos de danos provenientes de incêndio, enchente, terremoto, explosão, manifestações e outras formas de desastre natural ou provocado pelo homem.
- 1.5.6. O Fornecedor deverá assegurar que dentro das instalações do Fornecedor as pessoas (por exemplo, empregados, visitantes, contratados residentes) possam ser identificadas imediatamente (por exemplo, utilizando crachá, reconhecimento visual ou outros meios).
- 1.5.7. As instalações do Fornecedor que contenham Sistemas de Servidores ou Aplicações Dentro do Escopo que armazenem, processem, ou transmitam Informação Altamente Restrita da Johnson & Johnson deverão ter todos os pontos de entrada/saída das instalações monitorados pela equipe de segurança e/ou registrados com câmeras de segurança vinte e quatro (24) horas por dia, sete (7) dias por semana. As gravações da câmera de segurança deverão ser armazenadas por não menos de noventa (90) dias.
- 1.5.8. As instalações do Fornecedor que contenham Sistemas de Servidor ou Aplicações Dentro do Escopo que armazenem, processem, ou transmitam Informação Restrita da Johnson & Johnson ou Informação Altamente Restrita da Johnson & Johnson deverá possuir todos os pontos de entrada/saída do data center monitorados pela equipe de segurança e/ou registrados com câmeras de segurança vinte e quatro (24) horas por dia, sete (7) dias por semana. As gravações da câmera de segurança deverão ser armazenadas por não menos de noventa (90) dias.
- 1.5.9. O Fornecedor deverá arquivar e trancar Informação Classificada da Johnson & Johnson em papel que não estiver em uso.
- 1.5.10. O Fornecedor deverá acompanhar visitantes durante todo o tempo onde Informação Classificada da Johnson & Johnson ou o acesso à rede interna do Fornecedor for prontamente acessível. Os data centers do Fornecedor deverão possuir um registro único para visitantes e manter um registro de controle de acesso.
- 1.5.11. O Fornecedor deverá controlar as áreas de entrega e de carga e isolar essas áreas e a as áreas de armazenamento dos data centers, se possível, a fim de evitar acesso não autorizado.

SEGURANÇA DE EQUIPAMENTOS

- 1.5.12. O Fornecedor deverá proteger os Sistemas, Dispositivos de Rede e outros equipamentos a fim de reduzir o risco de ameaças e perigos do ambiente e de oportunidades para acesso não autorizado.
- 1.5.13. O Fornecedor deverá assegurar que todos os Sistemas e Dispositivos de Rede utilizados para processar ou armazenar Informação Classificada da Johnson & Johnson estejam protegidas contra roubo, perda e acesso não autorizado.
- 1.5.14. O Fornecedor deverá proteger os equipamentos que sejam dependentes de energia contra queda e surtos de energia, e de outras anomalias elétricas.
- 1.5.15. O Fornecedor deverá assegurar que todo o cabeamento de energia, telefonia e rede seja protegido contra acesso não autorizado e danos.
- 1.5.16. O Fornecedor deverá manter os Recursos Computacionais de Rede e outros equipamentos a fim de assegurar sua contínua disponibilidade e integridade.
- 1.5.17. O Fornecedor deverá possuir procedimentos de saída adequados e implementados a fim de controlar a remoção não autorizada de Sistemas de Servidores e de Dispositivos de Rede.
- 1.5.18. O Fornecedor deverá verificar todos os Sistemas e Dispositivos de Rede que possam conter Informação Classificada da Johnson & Johnson a fim de assegurar que tal informação tenha sido removida de forma segura antes do descarte.

1.6. GESTÃO DE COMUNICAÇÕES E DE OPERAÇÕES

PROCEDIMENTOS E RESPONSABILIDADES OPERACIONAIS

- 1.6.1. O Fornecedor deverá possuir procedimentos de operação e listas de verificação de suporte padronizados e implementados para a gestão operacional de Sistemas, das Aplicações Dentro do Escopo e de Dispositivos de Rede que enderecem estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores.
- 1.6.2. O Fornecedor deverá possuir um processo de gestão de mudanças e procedimentos de suporte documentados e implementados a fim de controlar todas as mudanças nos Recursos Computacionais e de Rede.
- 1.6.3. O Fornecedor deverá segregar funções e áreas de responsabilidade a fim de reduzir as oportunidades para modificação não autorizada ou não intencional ou mau uso dos ativos do Fornecedor. A segregação de funções deverá estar documentada.
- 1.6.4. O Fornecedor deverá separar os ambientes de desenvolvimento, teste e operação/produção a fim de reduzir o risco de acesso não autorizado ou de alterações no sistema operacional ou na informação.

PLANEJAMENTO E ACEITAÇÃO DE SISTEMA

- 1.6.5. O Fornecedor deverá estabelecer critérios de aceitação para novos Sistemas e Dispositivos de Rede durante o desenvolvimento e antes da entrada em produção.
- 1.6.6. O Fornecedor deverá completar os Padrões de Configuração de Segurança ou os documentos de “hardening” para todos os Sistemas de Servidores, Aplicações Dentro do Escopo e Dispositivos de Rede antes de colocá-los em produção a fim de assegurar sua aderência a estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores e às melhores práticas da indústria.

PROTEÇÃO CONTRA CÓDIGO MALICIOSO E CÓDIGO MÓVEL

O Fornecedor deverá implementar os seguintes controles para software malicioso e código móvel:

- 1.6.7. Software anti-malware disponível comercialmente deverá ser instalado, configurado adequadamente e executado o tempo todo em Sistemas de Usuários e Sistemas de Servidores. O software deverá ser configurado para proteger contra todas as ameaças conhecidas, incluindo, mas não se limitando a vírus, cavalos de Troia, rootkits, spyware e keystroke loggers.
- 1.6.8. Nos casos em que o software anti-malware possui alerta, todas as detecções de malware deverão ser automáticas e imediatamente reportadas à equipe diretamente responsável pelo dispositivo infectado, a qual deverá endereçar o alerta e a causa raiz.
- 1.6.9. Quando houver detecção de software ou conteúdo malicioso, o malware deverá ser imediatamente posto em quarentena, bloqueado, desabilitado, confiscado ou de alguma forma interrompido a fim de assegurar que não será propagado. A detecção e a coleta de evidências deverão estar aderentes a todas as leis aplicáveis e às regulamentações do governo.
- 1.6.10. Os dispositivos deverão ser examinados de acordo com a tabela a seguir, sem intervenção humana.

Classe de Dispositivo	Proteção em Tempo real	Scan Periódico	Scan Sob Demanda
Desktops / Laptops/ Estações de Trabalho (Por exemplo, Windows e MacOS)	Habilitada para todos os arquivos em todos os sistemas de arquivos locais, e somente os sistemas de arquivos locais	Semanalmente para todos os arquivos em sistemas de arquivos locais, e somente os sistemas de arquivos locais	Capaz de executar um scan de quaisquer ou todos os arquivos
Dispositivos Móveis (por exemplo, smartphones, tablets executando iOS, Android, ou Blackberry OS)		A disponibilidade e necessidade de Anti-Malware deverá ser avaliada para cada dispositivo e/ou sistema operacional, considerando as ameaças e outros controles que mitiguem o risco. O Information Security Officer deverá prover a decisão sobre a necessidade como parte da aprovação de segurança sobre o projeto de apoio.	
Servidores (por exemplo, Windows, Unix, Linux)	Habilitada para arquivos executados localmente	Semanalmente para sistemas operacionais e arquivos executáveis de aplicação no sistema de arquivos local	Capaz de executar um scan dos sistemas de arquivos locais

- 1.6.11. Além dos requisitos de scan listados acima, servidores, ferramentas e serviços em quaisquer dos Papéis especificados abaixo deverão possuir também as seguintes configurações de scan, mesmo que o scan não seja requerido acima.

Papel do Dispositivo	Proteção em Tempo Real	Scan Periódico	Scan Sob Demanda
----------------------	------------------------	----------------	------------------

Servidores, Ferramentas e Serviços de Armazenamento de Arquivos de Usuário Final	Não requerido	Semanalmente para todos os arquivos de usuário final armazenados no sistema de arquivos local	Capaz de iniciar um scan de quaisquer ou de todos os arquivos de usuário final armazenados no sistema de arquivos local
Servidores, Ferramentas e Serviços de Compartilhamento de Arquivos e de Colaboração (por exemplo, SharePoint)	O Information Security Officer deverá prover a decisão sobre a necessidade como parte da aprovação de segurança sobre o projeto de apoio	Semanalmente para todos os arquivos de usuário final armazenados no sistema de arquivos local	Capaz de iniciar um scan de quaisquer ou de todos os arquivos de usuário final armazenados no sistema de arquivos local
Plataforma de Aplicação e Ferramentas de Bancos de Dados (por exemplo, Teradata, SAP Hana, etc.)		A disponibilidade e necessidade de Anti-Malware deverá ser avaliada para cada ferramenta e/ou sistema operacional, considerando as ameaças e outros controles que mitiguem o risco. O Information Security Officer deverá prover uma decisão sobre a necessidade como parte da aprovação de segurança sobre o projeto de apoio	
Servidores, Ferramentas e Serviços de Email	Habilitados para mensagens e anexos de e-mails que chegam Enabled for e-mail ao ou são transmitidas através do gateway ou servidor de e-mail	Não requerido	Capaz de iniciar um scan de quaisquer ou de todos os arquivos armazenados no sistema de arquivos local

- 1.6.12. O software anti-malware, incluindo patches, atualizações de versão e atualizações de mecanismo deve ser mantido atualizado.
- 1.6.13. Os arquivos de definição de assinatura anti-malware devem ser atualizados dentro de 72 horas após a liberação pelo fornecedor para todos os sistemas.
- 1.6.14. Se o Fornecedor realizar assinatura de código (por exemplo, objetos ActiveX), o Fornecedor deverá ter um procedimento de assinatura de código documentado que cubra a aprovação, proteção de chave particular e uso aceitável.

BACK-UP

O Fornecedor deverá implementar os seguintes controles de backup:

- 1.6.15. Os backups de Dados deverão ser executados com base nos requisitos de negócio a fim de maximizar a disponibilidade dos dados e evitar a perda da Informação da Johnson & Johnson no caso de os dados originais ficarem indisponíveis.
- 1.6.16. Os backups e os eventos de recuperação de Dados deverão ser registrados.
- 1.6.17. Os backups de dados deverão ser executados imediatamente antes de quaisquer atividades de atualização ou manutenção de sistema.
- 1.6.18. Os Dados da Johnson & Johnson que requerem encriptação no armazenamento por estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores deverão continuar encriptados durante todo o processo de backup de Dados.

- 1.6.19. Os backups de Dados deverão ser armazenados em instalações geograficamente separadas e fisicamente seguras.
- 1.6.20. O Fornecedor deverá testar a capacidade de restauração dos backups de Dados, no mínimo, anualmente e fornecer à Johnson & Johnson os resultados dos testes quando requerido.

GESTÃO DE SEGURANÇA DE REDE

O Fornecedor deverá implementar os seguintes controles para a gestão da segurança de rede:

- 1.6.21. Deverá existir um firewall a fim de proteger o acesso à rede do Fornecedor. O(s) firewall(s) deverá(ão) definir e aplicar regras sobre a informação e os usuários que trafegam entre os sistemas internos e externos.
- 1.6.22. As regras do firewall deverão permitir ou negar conexão tanto de saída quanto de entrada. O acesso que não for explicitamente permitido deverá ser negado.
- 1.6.23. Todos os acessos permitidos pelo firewall e todas as alterações de hardware, software e de configuração do firewall deverão possuir um objetivo de negócio documentado e uma avaliação de risco associada e deverão ser aprovadas pelo Information Security Officer do fornecedor ou seu delegado.
- 1.6.24. Qualquer sessão administrativa direta ou remota em um firewall não deve mostrar o último usuário a efetuar login e deverá ser desconectada se estiver inativa.
- 1.6.25. Os firewalls de hardware interno (quando utilizados) que protegem Informação Classificada da Johnson & Johnson deverão ser configurados e gerenciados de acordo com estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores.
- 1.6.26. Os laptops, desktops e estações de trabalho do Fornecedor deverão possuir um software firewall instalado e configurado para bloquear todo o tráfego de entrada que não seja requerido pelos objetivos de negócio, e não deverá permitir sua desativação, alteração ou atualização por pessoal não autorizado.
- 1.6.27. Todas as conexões entre uma rede externa (incluindo, não se limitando à Internet) e a rede interna do Fornecedor terá de empregar funcionalidades de detecção (ou prevenção) de intrusão. Essas funcionalidades (doravante referidas como “IDS/IPS”) podem ser agrupadas em dispositivos de firewall e/ou em sistemas separados.
- 1.6.28. Os sistemas IDS/IPS não deverão ser desativados, deverão atualizar as assinaturas utilizadas para identificar comportamento malicioso, no mínimo, a cada 60 dias, deverão fornecer alertas quando eventos significativos forem identificados e deverão bloquear o tráfego anômalo quando possível.
- 1.6.29. Antes de realizar mudanças no perímetro da rede do Fornecedor (por exemplo, na conexão de Internet, adicionando um novo site físico à rede), o Fornecedor deverá realizar uma avaliação de risco, assegurar que a mudança atende as políticas aplicáveis (incluindo, mas não se limitando a estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores) e ser aprovada pelo Information Security Officer do Fornecedor ou seu delegado autorizado.

MANUSEIO DE MÍDIA

O Fornecedor deverá implementar os seguintes controles para manuseio de mídia:

- 1.6.30. O descarte de mídia (papel, filme ou eletrônica) contendo qualquer Informação Classificada da Johnson & Johnson deverá ser aprovado pela Johnson & Johnson ou pela Afiliada Johnson & Johnson aplicável e deverá utilizar práticas ou mecanismos de

destruição de mídia aprovados pela Johnson & Johnson ou por uma Afiliada da Johnson & Johnson, quando apropriado.

- 1.6.31. Informação Confidencial da Johnson & Johnson e Informação Restrita da Johnson & Johnson armazenada dentro de um Recurso Computacional e de Rede ou em um Dispositivo Removível de Armazenamento deverá ser protegida por encriptação (de forma aderente a estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores) ou por proteção física contra perda, roubo e acesso não autorizado.
- 1.6.32. Informação Altamente Restrita da Johnson & Johnson, incluindo Informação Pessoal Especial da Johnson & Johnson, deverá ser encriptada de forma aderente a estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores quando:
- a) a informação é armazenada dentro de Recursos Computacionais e de Rede do Fornecedor, de Aplicações Dentro do Escopo, ou de datastores (por exemplo, pasta de rede compartilhada) em que requisitos legais, regulatórios ou contratuais exijam encriptação; b) as informações são senhas; c) a informação é armazenada dentro de Sistemas de Usuários; ou d) a informação é armazenada em Dispositivos Removíveis de Armazenamento. Qualquer outra Informação Altamente Restrita da Johnson & Johnson armazenada dentro de Recursos Computacionais e de Rede do Fornecedor deverá ser protegida por encriptação (de forma aderente a estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores) e/ou por proteção física contra perda, roubo e acesso autorizado em aderência a estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores.

- Quando Informação Pessoal Especial for armazenada em Sistemas de Servidores, em Aplicações Dentro do Escopo (por exemplo, bancos de dados), datastores ou mídia de back-up e o Fornecedor não necessitar encriptar a informação devido ao descrito acima ou foi definido que a encriptação de tal informação não é possível, o Fornecedor deverá documentar os controles existentes para proteger tal informação de forma consistente com os requisitos legais locais e com os Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores, incluindo medidas para detectar possíveis violações de forma tempestiva, e deverá prover tal documentação quando solicitado pela Johnson & Johnson.

TROCA DE INFORMAÇÃO

- 1.6.33. O Fornecedor deverá possuir políticas, procedimentos e controles implementados para proteger a troca de Informação Classificada da Johnson & Johnson através de todos os tipos de mecanismos de comunicação.
- 1.6.34. O Fornecedor deverá encriptar Informação Restrita da Johnson & Johnson de forma aderente a estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores quando transmitida eletronicamente, incluindo a modalidade sem fio, através de quaisquer redes diferentes da rede do Fornecedor. O Fornecedor deverá encriptar a Informação Altamente Restrita da Johnson & Johnson de forma aderente a estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores quando transmitida eletronicamente através de quaisquer redes.
- 1.6.35. O Fornecedor deverá utilizar um serviço de transporte ou de entrega confiável ao transportar mídia física que contenha Informação Classificada da Johnson & Johnson e utilizar um empacotamento adequado para proteger o conteúdo.

- 1.6.36. O Fornecedor deverá possuir políticas e procedimentos implementados a fim de proteger a Informação da Johnson & Johnson associada à interconexão de sistemas de informação de negócio com quaisquer entidades externas.

MONITORAMENTO

O Fornecedor deverá implementar os seguintes controles para registro e monitoramento de auditoria:

- 1.6.37. O registro de auditoria deverá ser ativado nos Dispositivos de Rede, Sistemas de Servidores que contenham Informação da Johnson & Johnson, Aplicações Dentro do Escopo e todos os sistemas e ferramentas relacionados à segurança (por exemplo, sistemas de gestão de identidade, controladores de domínio, servidores de gestão de anti-malware, etc.), quando suportados pelo sistema de coleta de registros, a fim de capturar, no mínimo, os eventos relativos à segurança definidos a seguir:
- Logon de conta (tanto bem-sucedido como malsucedido) e logoff
 - Tentativas de acesso com falha
 - Bloqueios de conta
 - Elevação de privilégios (tanto bem-sucedido como malsucedido), e todo uso de privilégio elevado ou ações tomadas enquanto o privilégio esteve elevado
 - Criação, modificação e exclusão (tanto bem-sucedida como malsucedida) de:
 - o Identificadores de contas ou de logon
 - o Associação a grupos
 - o Privilégios/atributos de acesso para contas e grupos
 - o Direitos e permissões de usuário
 - Mudanças no status de conta ou de logon (tanto bem-sucedidas como malsucedidas)
 - Modificações, ou tentativas não autorizadas de modificação, da configuração de segurança, função de segurança ou da política de autorização
- 1.6.38. Os registros de auditoria deverão capturar, no mínimo, as informações definidas a seguir para cada evento relacionado à segurança:
- Identificador dos usuários, do sistema ou do processo que disparou um evento
 - Descrição do evento
 - Data e hora da ocorrência do evento (a data e a hora têm de ser sincronizadas periodicamente a fim de assegurar sua acurácia)
 - Identificador do sistema que gerou o evento (por exemplo, endereço IP)
 - Informação de autorização associada ao evento
- 1.6.39. Os registros de auditoria deverão ser retidos por não menos de noventa (90) dias.
- 1.6.40. Os registros de auditoria e/ou relatórios de erro deverão ser revisados, no mínimo, semanalmente para sistemas críticos (controladores de domínio, gateways de acesso remoto, etc.) e, no mínimo, mensalmente para todos os outros sistemas.
- 1.6.41. Os registros de auditoria deverão ser protegidos contra modificação ou destruição acidental ou intencional e os Recursos Computacionais e de Rede deverão ser automaticamente sincronizados com uma fonte confiável de tempo.
- 1.6.42. Os eventos e alertas aplicáveis do IDS/IPS e outros alertas/eventos de segurança gerados por outros Recursos Computacionais e de Rede deverão ser tratados de acordo com os processos de monitoramento, reporte e resposta de incidentes de segurança do Fornecedor.

1.7. CONTROLE DE ACESSO

REQUISITOS DE NEGÓCIO PARA CONTROLE DE ACESSO

- 1.7.1. O Fornecedor deverá possuir uma política de controle de acesso e limitar o acesso autorizado de empregados, contratados e outros indivíduos às instalações, às áreas seguras e aos Recursos Computacionais e de Rede do Fornecedor a apenas aqueles indivíduos com os quais possua um acordo de confidencialidade válido e vigente e uma necessidade de negócio para o acesso.
- 1.7.2. A gerência do Fornecedor deverá aprovar o acesso de cada indivíduo para acesso às instalações, às áreas seguras (por exemplo, data centers, cabines de telecomunicação, etc.) e aos Recursos Computacionais e de Rede a fim de evitar acesso não autorizado.
- 1.7.3. O Fornecedor deverá ser capaz de gerenciar identidades e controlar acessos o suficiente para atender a estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores.
- 1.7.4. Os controles de acesso deverão exigir identificação positiva e autenticação dos indivíduos. Os processos de autenticação biométrica não deverão ser utilizados como único meio para autenticar um indivíduo aos Recursos Computacionais e de Rede.

GESTÃO DE ACESSO DE USUÁRIO

O Fornecedor deverá cumprir com os controles de gestão de acesso de usuário a seguir:

- 1.7.5. Os privilégios concedidos a um indivíduo deverão formar o conjunto mínimo requerido para a execução adequada e eficiente de suas funções e apenas durante o tempo necessário.
- 1.7.6. A gerência deverá aprovar ou negar todas as solicitações de privilégios elevados, conforme aplicável, de acordo com estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores.
- 1.7.7. Os indivíduos deverão ser solicitados a autenticar-se antes de atuar com quaisquer privilégios elevados (embora a mesma identidade e o mesmo meio de autenticação possa ser utilizado).
- 1.7.8. Os privilégios elevados deverão ser gerenciados ativamente e para tanto deverá haver revisão periódica de privilégios e revogação quando não mais forem necessários.
- 1.7.9. As senhas requeridas para autenticação deverão estar aderentes a estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores.
- 1.7.10. Senhas, PINs e outras informações utilizadas para autenticação (por exemplo, frases de segurança) sempre deverão estar encriptados de acordo com estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores, com as seguintes exceções:
 - As senhas iniciais ou PINs não precisam ser encriptados quando transmitidos através da rede do Fornecedor com troca requerida na primeira utilização.
 - As senhas de contas de serviço (ou seja, senhas atribuídas a um Sistema ou Aplicação Dentro do Escopo) não necessitam estar encriptadas nos arquivos de comando, de inicialização, ou de configuração quando o acesso a tais arquivos estiver restrito aos controles do sistema operacional e o sistema estiver fisicamente protegido nas instalações do Fornecedor.
- 1.7.11. As senhas e os PINs deverão ser entregues de maneira confidencial de forma que exija o destinatário comprovar sua identidade antes de receber a senha e/ou o PIN.

- 1.7.12. As senhas e os PINs nunca deverão ser entregues com o respectivo ID de Usuário através do mesmo meio e no mesmo momento a menos que a confidencialidade da entrega e a prova da identidade do destinatário sejam realizadas utilizando-se o padrão de criptografia de chave pública da indústria.
- 1.7.13. Senhas/PINs temporários, reiniciados ou iniciais deverão ser únicos para cada indivíduo, deverão exigir a troca da senha na primeira utilização e não deverão ser reutilizados por, no mínimo, três (3) meses.
- 1.7.14. A prova adequada de identificação deverá ser fornecida e verificada antes da troca da senha ou PIN.
- 1.7.15. Senhas/PINs default deverão ser alterados durante ou imediatamente quando da conclusão do processo de instalação.
- 1.7.16. Contas comprometidas e contas suspeitas de terem sido comprometidas deverão ser desabilitadas em até vinte e quatro (24) horas.
- 1.7.17. Quando ocorrer o desligamento de um indivíduo, a conta do indivíduo deverá ser desabilitada e todas as senhas e PINs sob o controle deste indivíduo (por exemplo, senha de conta de serviço) deverá ser alterada em, no máximo, 72 horas após seu desligamento.
- 1.7.18. O Fornecedor deverá revisar e reaprovar os privilégios a cada seis meses para Sistemas contendo Informação Classificada da Johnson & Johnson e Aplicações Dentro do Escopo e, anualmente, para outros Sistemas. Eventos como alterações no título ou papel deverão disparar revisões e reaprovações adicionais.

RESPONSABILIDADE DO USUÁRIO

- 1.7.19. O Fornecedor deverá deixar os usuários cientes dos requisitos de segurança para a escolha e uso de senhas e PINs, e de que devem mantê-los em sigilo.
- 1.7.20. O Fornecedor deverá deixar os usuários cientes da necessidade de arquivar e trancar documentos em papel e dispositivos portáteis de armazenamento que contenham Informação Classificada da Johnson & Johnson quando não estiverem em uso.
- 1.7.21. O Fornecedor deverá treinar os indivíduos ou torná-los cientes sobre não deixarem os Recursos Computacionais e de Rede com sua interface desbloqueada quando não estiverem em uso.

CONTROLE DE ACESSO À REDE

O Fornecedor deverá implementar os seguintes controles de acesso à rede:

- 1.7.22. O Fornecedor deverá limitar o acesso à rede do Fornecedor a apenas aqueles empregados, contratados e outros usuários que tenham uma necessidade de negócio para o acesso.
- 1.7.23. Todas as sessões de comunicação através de acesso remoto ou de rede sem fio deverão utilizar protocolos de rede que protejam a confidencialidade e a integridade de todos os dados em trânsito. Esses protocolos deverão estar aderentes a todos os padrões de criptografia para algoritmos e tamanhos de chave especificados nestes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores.
- 1.7.24. Todos os serviços via acesso remoto ou de rede sem fio que conceda acesso irrestrito à rede do Fornecedor deverá assegurar que o indivíduo que busca por serviços seja identificado e fortemente autenticado antes de obter acesso.
 - Acesso remoto à rede do Fornecedor que permita acesso ou à Informação Restrita da Johnson & Johnson, ou à Aplicações Dentro do Escopo contendo Informação Restrita da Johnson & Johnson deverão empregar duplo fator de autenticação utilizando: a) um token

físico ou protegido que contenha materiais criptográficos combinados com uma senha ou outro fator que somente o usuário conheça; b) uma senha segura combinada com um código de segurança de não reutilizável de um Fornecedor de serviço aprovado.

- O acesso à rede do Fornecedor através da rede sem fio interna às suas instalações ou o acesso remoto à rede do Fornecedor que forneça acesso à Informação Confidencial da Johnson & Johnson ou à Informação Restrita da Johnson & Johnson, ou acesso a Sistemas de Servidor ou a Aplicações Dentro do Escopo que contenham Informação Confidencial da Johnson & Johnson ou Informação Restrita da Johnson & Johnson, deverá empregar duplo fator de autenticação utilizando: a) um token físico ou protegido que contenha materiais criptográficos combinados com uma senha ou outro fator que somente o usuário conheça; ou b) uma senha segura combinada com um código de segurança não reutilizável de um Fornecedor de serviço aprovado.

- 1.7.25. O acesso direto de diagnóstico aos Sistemas do Fornecedor ou suas redes com o objetivo de monitorar ou diagnosticar e/ou reparar problemas não deverá permitir:
 - Privilégios elevados ou de administrador sem uma ativação explícita e a supervisão de equipe autorizada;
 - O acesso a quaisquer outras localidades ou serviços na rede do Fornecedor; nem
 - O acesso às redes ou à Informação da Johnson & Johnson.
- 1.7.26. Nenhum Sistema de Usuário deverá estar conectado a mais de uma rede simultaneamente de forma a permitir o roteamento o tráfego entre as redes.
- 1.7.27. Equipamento de áudio ou audiovisual de teleconferência deverá estar configurado para não responder quaisquer conexões de entrada sem ação humana para estabelecer uma conexão.

CONTROLE DE ACESSO ao SISTEMA OPERACIONAL e à APLICAÇÃO DENTRO DO ESCOPO

O Fornecedor deverá implementar os seguintes mecanismos de controle de acesso para todos os sistemas operacionais de Sistemas de Usuário, Sistemas de Servidor e Dispositivos de Rede e para todas as Aplicações Dentro do Escopo:

- 1.7.28. Os controles de acesso deverão exigir identificação individual e autenticação dos usuários. Os processos de autenticação biométrica não deverão ser utilizados como o único meio de autenticação a um indivíduo, exceto para permitir o desbloqueio de um Dispositivo Computacional Móvel em que o mecanismo de biométrica tenha sido avaliado e aprovado pelo Information Security Officer do Fornecedor.
- 1.7.29. As decisões de autorização deverão basear-se na identidade autenticada do indivíduo e nos privilégios concedidos àquele indivíduo.
- 1.7.30. Os privilégios de acesso de usuário deverão ser desabilitados quando não forem utilizados por 180 dias a menos que uma revisão da lista de controle de acesso seja executada a cada 180 dias e as contas que não mais requeiram acesso sejam desabilitadas.
- 1.7.31. Senhas individuais deverão exigir um tamanho de, pelo menos, 8 caracteres e conter caracteres de, pelo menos, duas classes de complexidade (maiúsculas, minúsculas, números, caracteres especiais) ou exigir um tamanho de, pelo menos, seis caracteres e conter caracteres de, pelo menos, três classes de complexidade. Os Dispositivos Computacionais Móveis que contenham, ou que sejam utilizados para acessar Informação Classificada da Johnson & Johnson deverão exigir uma senha para obter acesso e essa senha deverá exigir um tamanho de, pelo menos, seis caracteres.
- 1.7.32. As senhas de conta de serviço deverão exigir um tamanho de, pelo menos, dez caracteres e conter caracteres de, pelo menos, três classes de complexidade.

- 1.7.33. As senhas e PINs individuais têm de expirar e serem trocadas a cada 90 dias. As senhas de contas de serviço podem possuir um período maior para expirarem conforme definido pelo Fornecedor. As senhas e PINs não podem ser reutilizados nem em 365 dias, nem antes da quinta troca.
- 1.7.34. Cinco (5) tentativas falhas consecutivas para autenticar-se utilizando uma senha dentro de um período de quinze (15) minutos deverão resultar no bloqueio da conta ou sua desativação temporária por, pelo menos, quinze (15) minutos.
- 1.7.35. Quando tecnicamente possível, os nomes das contas padrões deverão ser alterados.
- 1.7.36. Excetuando-se os Dispositivos Computacionais Móveis, a autenticação por senha deverá assegurar que as senhas/PINs não sejam apresentadas aos indivíduos de forma legível em momento algum. Os Dispositivos Computacionais Móveis podem apresentar os caracteres individualmente de forma legível devendo tornar-se ilegível ao se inserir o caractere seguinte.
- 1.7.37. As senhas/PINs deverão ser alteradas sempre que houver indícios de terem sido descobertas.
- 1.7.38. As senhas e os PINs nunca deverão ser armazenadas em cache.
- 1.7.39. Excetuando-se as Aplicações Dentro do Escopo, a interface de usuário deverá ser bloqueada em até 15 minutos de inatividade e deverá exigir que o usuário se reautentique para desbloquear a interface.

COMPUTAÇÃO MÓVEL

O Fornecedor deverá implementar os seguintes controles para a computação móvel:

- 1.7.40. A aprovação da gerência do Fornecedor terá de ser obtida antes que o Sistema de Usuário seja utilizado para armazenar ou transmitir Informação Restrita da Johnson & Johnson ou Informação Altamente Restrita da Johnson & Johnson.
- 1.7.41. Os Sistemas de Usuários deverão estar fisicamente protegidos e deverão exigir autenticação por senha de acordo com os Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores, a qual não pode ser contornada.
- 1.7.42. Exceto se expressamente estabelecido nestes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores, um Dispositivo Computacional Móvel não tem tratamento diferente de qualquer Sistema de Usuário por estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores. Se um Dispositivo Computacional Móvel armazena ou transmite Informação Classificada da Johnson & Johnson, ele deverá encriptar a Informação Classificada da Johnson & Johnson em trânsito e no armazenamento de acordo com estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores.
- 1.7.43. Os Dispositivos Computacionais Móveis contendo Informações Classificadas da Johnson & Johnson deverão ser capazes de limpar a informação existente no dispositivo (por exemplo, apagar a informação ou assegurar que a chave criptográfica que protege a informação seja apagada) a partir de um comando remoto ou após dez tentativas falhas consecutivas de autenticação no dispositivo. Os comandos de limpeza remota para apagar Informação Classificada da Johnson & Johnson deverão ser enviados quando o dispositivo for perdido ou roubado, ou quando for detectado que os controles de segurança foram burlados.

1.8. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

CONTROLES CRIPTOGRÁFICOS

O Fornecedor deverá implementar controles criptográficos para encriptação e outras funções criptográficas:

1.8.1. Os algoritmos e os tamanhos de chaves criptográficas a seguir são aceitáveis para todos os usos:

- Encriptação Simétrica: AES (128 bits ou acima), 3DES (112 bits ou acima)
- Encriptação Assimétrica e Assinatura Digital: RSA (2048 bits ou acima)
- Hashing: SHA-2 (tamanho da saída: 224 bits ou acima), ou SHA-3 (tamanho da saída: 224 bits ou acima)

O Fornecedor deverá obter a aprovação da Johnson & Johnson ou da Afiliada da Johnson & Johnson aplicável antes de utilizar outros algoritmos e tamanhos de chave. Se a Johnson & Johnson ou a Afiliada da Johnson & Johnson aplicável não fornecer sua aprovação, os algoritmos e tamanhos de chave acima deverão ser utilizados.

1.8.2. O hashing utilizando SHA2, ou SHA3 deverá ser considerado criptografia aceitável para armazenamento de senhas e PINs.

1.8.3. Cipher Suites com todas as características a seguir são aceitáveis para todos os usos:

- Deverá ser um cipher suite TLS
- Deverá especificar troca de chave por RSA **ou** Diffie-Hellman (com ou sem curva Elíptica e/ou variações efêmeras)
- Deverá especificar autenticação de endpoint RSA
- Deverá especificar encriptação de dados AES **ou** 3DES
- Deverá especificar um código de autenticação de mensagem SHA

O Fornecedor deverá obter a aprovação da Johnson & Johnson ou da Afiliada da Johnson & Johnson aplicável antes de utilizar outros Cipher Suites. Se a Johnson & Johnson ou a Afiliada Johnson & Johnson aplicável não fornecer sua aprovação, um dos Cipher Suites acima deverá ser utilizado.

1.8.4. O Fornecedor deverá possuir um processo e controles implementados a fim de assegurar que as chaves simétricas de encriptação e as chaves privadas assimétricas estejam encriptadas na transmissão e no armazenamento, sejam protegidas contra acesso não autorizado e estejam seguras.

1.8.5. A segregação de tarefas deverá ser instituída de tal forma que o pessoal administrativo com acesso de leitura às chaves seja distinto dos indivíduos com acesso de leitura ao texto cifrado.

1.8.6. Os sistemas que empregam chaves simétricas de encriptação deverão ser capazes de alterar/atualizar a(s) chave(s).

1.8.7. As chaves simétricas de encriptação definidas como padrão pelo fornecedor sempre deverão ser alteradas para valores diferentes do padrão, de tal forma que seus valores não sejam conhecidos por outros clientes do fornecedor, nem pelo fornecedor a menos que seja requerido por uma dada função.

1.8.8. As chaves simétricas de encriptação utilizadas para encriptar backups deverão ser armazenadas separadamente dos dados que estão sendo copiados em backup.

1.8.9. O Fornecedor deverá utilizar recursos de PKI de fornecedores confiáveis a fim de proteger a Informação Classificada da Johnson & Johnson e outras informações sensíveis (como, por exemplo, proteger as senhas com TLS durante a transmissão).

SEGURANÇA DOS ARQUIVOS DE SISTEMA

O Fornecedor deverá implementar os seguintes controles de segurança de sistema em todos os Recursos Computacionais e de Rede:

- 1.8.10. Todas as instalações de software em Sistemas de Usuário, Sistemas de Servidor e Dispositivos de Rede deverão ser avaliados, exigir uma análise de risco e ser aprovados pelo Information Security Officer do Fornecedor ou seu delegado.
- 1.8.11. As atualizações e correções de software deverão ser pesquisadas, testadas e verificadas pela equipe apropriada do Fornecedor antes da instalação.

SEGURANÇA NOS PROCESSOS DE DESENVOLVIMENTO E SUPORTE

- 1.8.12. O Fornecedor deverá possuir um Ciclo de Vida de Desenvolvimento de Sistema (System Development Lifecycle – SDLC) para o desenvolvimento e implementação dos Sistemas e das Aplicações Dentro do Escopo, que inclua atividades e entregáveis que assegurem que os requisitos de segurança sejam atendidos.
- 1.8.13. As práticas de codificação Segura deverão ser utilizadas para websites e aplicações web acessíveis pela Internet que armazenam Informação da Johnson & Johnson, incluindo, mas não se limitando a validação de entrada/saída, tratamento de erro e de exceção, criptografia, gestão de cookie e de sessão, e configuração de sistema (por exemplo, credenciais/arquivos default deverão ser removidos ou desativados).
- 1.8.14. O Fornecedor deverá executar testes a fim de assegurar que os requisitos de segurança sejam atendidos, incluindo o teste de interfaces entre sistemas e componentes de sistema.
- 1.8.15. O Fornecedor deverá assegurar que os dados de produção da Johnson & Johnson não sejam utilizados em ambientes de não-produção (por exemplo, desenvolvimento ou teste) a menos que os dados estejam protegidos conforme estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores.

GESTÃO TÉCNICA DE VULNERABILIDADE

O Fornecedor deverá implementar os seguintes controles de gestão técnica de vulnerabilidade:

- 1.8.16. Os proprietários de aplicação e de sistema deverão monitorar regularmente as fontes aplicáveis para informação relativa a boletins de segurança ou sobre a publicação de correções de segurança pelos fornecedores.
- 1.8.17. As correções críticas de segurança disponibilizadas pelo Fornecedor deverão ser aplicadas assim que viável, não ultrapassando os prazos abaixo, a menos que haja uma ameaça severa, iminente, ou imediata que exija que a correção seja aplicada imediatamente:
 - Sistemas de Usuário: em até 30 dias a partir da publicação pelo fornecedor.
 - Sistemas de Servidores acessíveis pela Internet: em até 30 dias a partir da publicação pelo fornecedor.
 - Todos os outros Sistemas de Servidores: em até 90 dias a partir da publicação pelo fornecedor.
 - Aplicações Dentro do Escopo: em até 1 ano a partir da publicação pelo fornecedor.
 - Dispositivos de Rede: em até 30 dias da publicação pelo fornecedor.
- 1.8.18. Correções de segurança não-críticas disponibilizadas pelo Fornecedor deverão ser aplicadas assim que viável, não ultrapassando os seguintes prazos:
 - Sistemas de Usuário: em até 30 dias a partir da publicação do fornecedor.
 - Sistemas de Servidores acessíveis pela Internet: em até 90 dias a partir da publicação do fornecedor.

- Todos os outros Sistemas de Servidores: em até 1 ano a partir da publicação do fornecedor.

- Aplicações Dentro do Escopo: em até 1 ano a partir da publicação do fornecedor.

- Dispositivos de Rede: em até 90 dias a partir da publicação do fornecedor.

1.8.19. O Fornecedor deverá utilizar uma ferramenta padrão de mercado para varredura de vulnerabilidade a fim de executar varreduras de vulnerabilidades nos Sistemas de Servidores e Dispositivos de Rede acessíveis pela Internet antes de mover tais Sistemas de Servidores/Dispositivos de Rede para a produção. As vulnerabilidades identificadas no teste da pré-produção deverão ser remediadas antes de mover o Sistema de Servidor ou o Dispositivo de Rede para a produção.

1.8.20. O Fornecedor deverá utilizar uma ferramenta padrão de mercado para varredura de vulnerabilidade a fim de executar, mensalmente, varreduras de vulnerabilidades em todos os Sistemas de Servidores e Dispositivos de Rede de produção. As vulnerabilidades identificadas nos sistemas de produção deverão ser remediadas assim que viável, não ultrapassando o prazo de 60 dias após a identificação da vulnerabilidade.

1.8.21. O Fornecedor deverá utilizar uma ferramenta padrão de mercado para varredura de vulnerabilidade a fim de executar varreduras de vulnerabilidades tanto nas Aplicações Dentro do Escopo baseadas em web acessíveis pela Internet na pré-produção, quanto nos websites acessíveis pela Internet na pré-produção que armazenem Informação da Johnson & Johnson Information, pelo menos, para os atuais dez riscos de segurança mais comuns do Projeto Aberto de Segurança de Aplicações Web (Open Web Application Security Project – “OWASP Top 10”), localizado em www.owasp.com. As vulnerabilidades identificadas na varredura da pré-produção deverão ser remediadas antes de mover a aplicação ou o website para a produção. Um relatório por escrito deverá ser enviado à Johnson & Johnson de forma segura, pelo menos, cinco (5) dias úteis antes da entrada em produção indicando que tal vulnerabilidade ou risco não mais existe.

1.8.22. O Fornecedor deverá utilizar uma ferramenta padrão de mercado para varredura de vulnerabilidade a fim de executar, trimestralmente, varreduras de vulnerabilidades no ambiente de produção tanto nas Aplicações Dentro do Escopo acessíveis pela Internet, quanto nos websites acessíveis pela Internet que armazenem Informação da Johnson & Johnson, pelo menos, para os “OWASP Top 10”. Um relatório por escrito deverá ser enviado à Johnson & Johnson de forma Segura em até cinco (5) dias úteis após cada varredura, incluindo os resultados da varredura.

1.8.23. As vulnerabilidades identificadas nas aplicações ou nos websites de produção deverão ser remediadas assim que viável, não ultrapassando os seguintes prazos:

- As vulnerabilidades identificadas pela ferramenta de varredura como sendo de Risco Alto ou uma falha crítica que podem permitir que a aplicação ou o website seja explorado: em até 30 dias após a identificação da vulnerabilidade/falha. Além disso, sempre que a Johnson & Johnson solicitar, o Fornecedor deverá imediatamente remover ou bloquear o acesso ao website ou página web afetada até que a vulnerabilidade de Risco Alto seja remediada.

- As vulnerabilidades identificadas pela ferramenta de varredura como sendo de Risco Médio ou uma falha que apresente o potencial de exploração da aplicação ou do website: em até 60 dias após a identificação da vulnerabilidade/falha.

- As vulnerabilidades identificadas pela ferramenta de varredura como sendo de Baixo Risco ou uma falha que apresente potencial para exploração de aplicação ou de website: de acordo com as políticas e procedimentos internos do Fornecedor.

- 1.8.24. A Johnson & Johnson reserva o direito de executar, a qualquer momento, varreduras, não autenticadas, de vulnerabilidades de seu(s) website(s) hospedado(s) externamente. Os apontamentos serão endereçados pelo Fornecedor de acordo com a Seção 1.8.23.

1.9. GESTÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

- 1.9.1. O Fornecedor deverá ser capaz de monitorar, reportar e responder formalmente a incidentes de segurança da informação a fim de identificar, reportar e responder adequadamente a incidentes confirmados ou suspeitas, incluindo qualquer acesso, aquisição, utilização, divulgação ou destruição não autorizada de Informação Pessoal da Johnson & Johnson. Esta capacidade deverá assegurar que a notificação seja enviada à Johnson & Johnson ou à Afiliada Johnson & Johnson aplicável em até 24 horas depois de qualquer confirmação ou suspeita de comprometimento da Informação da Johnson & Johnson ou de Aplicações Dentro do Escopo.
- 1.9.2. O Fornecedor deverá assegurar que um relatório de avaliação seja criado quando um Sistema de Usuário for perdido ou roubado, identificando o comprometimento ou potencial comprometimento da informação. Se Informação Classificada da Johnson & Johnson, incluindo Informação Pessoal da Johnson & Johnson, estiver incluída no relatório de avaliação, o Fornecedor terá de notificar a Johnson & Johnson ou a Afiliada da Johnson & Johnson aplicável dentro de 24 horas.

1.10. GESTÃO DE CONTINUIDADE DE NEGÓCIO

- 1.10.1. O Fornecedor deverá identificar os requisitos, e implementar as práticas, para os Planos de Continuidade de Negócio (CoB) e Planos de Recuperação de Desastre (DRP) para os Sistemas de Informação que evitarão perda catastrófica de dados e que assegurarão a restauração em tempo adequado da rede e dos serviços computacionais no caso de falha, dano ou destruição de sistema.
- 1.10.2. O Fornecedor deverá assegurar que o Plano de CoB/DRP seja testado, pelo menos, uma vez a cada dois anos a fim de assegurar que possa ser corretamente e eficientemente executado.

1.11. CONFORMIDADE

- 1.11.1. O Fornecedor deverá estar aderente a quaisquer requisitos legais e regulatórios aplicáveis na execução de serviços para a Johnson & Johnson ou para qualquer Afiliada da Johnson & Johnson.
- 1.11.2. O Fornecedor deverá assegurar conformidade com as respectivas leis, regulamentações e cláusulas contratuais, incluindo conformidade aos Padrões de Segurança de Dados da Indústria de Cartões de Pagamento (PCI), a fim de assegurar a proteção da Informação Pessoal da Johnson & Johnson.
- 1.11.3. O Fornecedor deverá permitir e suportar a elaboração de avaliações periódicas pela Johnson & Johnson ou por uma Afiliada da Johnson & Johnson a fim de determinar a conformidade com estes Requisitos de Segurança da Informação da Johnson & Johnson para Fornecedores.