# Padrão de Segurança da Informação (ISS)

## 1. Finalidade

Este Padrão de Segurança de Informações (“ISS”) estabelece os requisitos de segurança de informações da Eli Lilly and Company e suas afiliadas ("Lilly") para terceiros/fornecedores (cada um, "Terceiro/Fornecedor") com relação à confidencialidade, integridade e disponibilidade de Informações (definidos abaixo). Quaisquer obrigações adicionais de Terceiro/Fornecedor relacionadas à segurança da informação sob qualquer contrato com a Lilly são adicionais aos requisitos deste Padrão de Segurança da Informação.

Para esclarecimento, este Padrão de Segurança da Informação se aplica a todas as Informações tratadas por um Terceiro/Fornecedor, incluindo tratamento por: (i) criação; (ii) edição; (iii) gestão; (iv) processamento; (v) acesso; (vi) recebimento; (vii) transferência; (viii) destruição; (ix) armazenamento; e/ou (x) hospedagem, em qualquer formato, incluindo, mas não se limitando a: (a) sistemas; (b) ambientes de nuvem; (c) ambientes de produção e não produção; (d) ativos e dispositivos eletrônicos (incluindo fornecidos pela Lilly e/ou aqueles de propriedade do Terceiro/Fornecedor denominados como "traga seu próprio dispositivo"); e (e) versões impressas.

## 2. Definições

As definições abaixo são para os fins desta Padrão de Segurança de Informações. Quaisquer termos em maiúsculas não definidos terão o significado que lhes é atribuído no contrato firmado com o Terceiro/Fornecedor (“Contrato”).

"**Informações Confidenciais**" significa Informações consideradas confidenciais ou de propriedade por uma parte do Contrato (a "Parte Reveladora"), incluindo Informações consideradas confidenciais ou proprietárias em virtude das obrigações da Parte Reveladora para com outra Pessoa, que podem ser divulgadas ou adquiridas por ou em nome da outra parte (a "Parte Receptora") ou que podem ser criadas pela Parte Receptora com base em uma divulgação de tais Informações recebidas da Parte Reveladora. Para fins do Contrato, as Informações Confidenciais podem incluir qualquer informação sobre o Contrato, incluindo sua existência, planos de pesquisa e desenvolvimento e resultados; novos compostos e processos; procedimentos de avaliação (incluindo testes clínicos e de campo); formulações de produtos; métodos de fabricação; aplicações a autoridades governamentais; precificação ou custo; planos de construção; estudos e planos de vendas, marketing e publicidade; listas de clientes; informação e software informático; técnicas especiais exclusivas para o negócio da Lilly; informações sujeitas a um direito de privacidade, inclusive sob a Lei Aplicável; Segredos de Negócio; informações que a Lilly mantém sob um sistema de proteção contra acesso não autorizado; e Informações Pessoais. O status das informações como Informações Confidenciais não é afetado pelos meios de aquisição ou divulgação. Por exemplo, as Informações Confidenciais podem ser adquiridas por comunicação escrita, oral ou eletrônica; diretamente do Representante da Parte Reveladora ou contratante independente, ou indiretamente por meio de um ou mais intermediários; ou por observação visual. Da mesma forma, a aquisição ou divulgação de informações pode ser intencional ou inadvertida, sem afetar seu status como Informação

# Padrão de Segurança da Informação (ISS)

Confidencial. Não obstante qualquer disposição em contrário no Contrato, as Informações Confidenciais (exceto Informações Pessoais) não incluem qualquer informação que:

(a) Seja geralmente conhecido do público ou se torne geralmente conhecido do público por outros meios que não a violação pela Parte Receptora de um dever contratual, legal ou fiduciário de confidencialidade devido à Parte Reveladora, suas Afiliadas, seus Subcontratados (se aplicável) ou qualquer um de seus Representantes;

(b) A Parte Receptora possuía legalmente antes de adquiri-la como resultado do Contrato;

(c) Esteja ou se torne disponível para a Parte Receptora em uma base não confidencial de uma terceira pessoa que, ao conhecimento da Parte Receptora após a devida investigação, não esteja vinculada a qualquer dever contratual, legal ou fiduciário de confidencialidade para com a Parte Reveladora, suas Afiliadas ou os Representantes da Parte Reveladora ou suas Afiliadas; ou

(d) É desenvolvido inteiramente por Representantes da Parte Receptora que não têm acesso às Informações Confidenciais da Parte Divulgadora.

"**Informações Pessoais**" significa qualquer informação, fornecida pela Lilly ou coletada pelo Terceiro/Fornecedor para a Lilly, relacionada a um Titular de Dados, que possa ser associada a uma pessoa ou seu domicílio. As Informações Pessoais podem estar em qualquer mídia ou formato, incluindo registros informatizados ou eletrônicos, bem como arquivos impressos. As Informações Pessoais incluem, mas não se limitam a: (i) um nome ou sobrenome ou iniciais; (ii) um endereço residencial ou outro endereço físico; (iii) um endereço de e-mail ou outras informações de contato on-line; (iv) um número de telefone; (v) um número de segurança social, número de identificação fiscal, número de identificação individual ou outro identificador emitido pelo governo; (vi) um endereço IP ou nome de host; (vii) um identificador persistente, como um número de cliente mantido em um "cookie" ou número de série do processador, que é combinado com outros dados disponíveis que identificam um indivíduo; (viii) datas de nascimento ou datas de tratamento; ou (ix) dados codificados derivados de Informações Pessoais. Além disso, na medida em que quaisquer outras informações, tais como, mas não limitado a informações de formulário de relato de caso, códigos de identificação de ensaios clínicos, informações de perfil pessoal, outros identificadores exclusivos ou informações biométricas sejam processadas, essas informações também serão consideradas Informações Pessoais. Para evitar dúvidas, as Informações Pessoais que tenham sido pseudonimizadas, o que significa que as informações não podem ser atribuídas a uma pessoa física sem o uso de informações adicionais, também serão consideradas Informações Pessoais.

"**Informações**" para fins deste Padrão de Segurança da Informação engloba Informações Confidenciais e Informações Pessoais que são usadas para fins comerciais (doravante denominadas de forma independente e/ou coletivamente aqui como "Informações").

# Padrão de Segurança da Informação (ISS)

## 3. Políticas e procedimentos de segurança da informação

O Terceiro/Fornecedor deve possuir e cumprir políticas, padrões e procedimentos de segurança da informação documentados para estabelecer seu ambiente de controle relacionado à proteção da confidencialidade, integridade e disponibilidade das Informações. Políticas e procedimentos devem ser revisados, atualizados e aprovados pela alta administração anualmente.

Se o uso de dispositivos pessoais para acessar informações ou sistemas for permitido pela Lilly ao Terceiro/Fornecedor, uma política de "traga seu próprio dispositivo" deve ser implementada por este último.

## 4. Governança e Treinamento

O pessoal do Terceiro/Fornecedor deve concluir um treinamento de segurança da informação relevante com requisitos para proteção e manuseio seguro das informações. Um resumo do treinamento concluído deve ser disponibilizado à Lilly mediante solicitação desta.

O Terceiro/Fornecedor deve fornecer um representante como ponto único de contato para todos os itens relacionados à segurança da informação. Além disso, o Terceiro/Fornecedor deve ter um representante designado que será responsável por supervisionar o cumprimento deste Padrão de Segurança da Informação.

## 5. Práticas de Segurança de Recursos Humanos

De acordo com o objeto da contratação, o Terceiro/Fornecedor se compromete a realizar triagem de pré-contratação, incluindo verificação de antecedentes criminais (quando permitido pela legislação local), revisão do currículo, revisão de credenciais e experiência, além de condução de entrevista para fins de alocar os profissionais adequados que trabalharão com as Informações.

O Terceiro/Fornecedor se obriga a firmar acordos de confidencialidade, não divulgação ou equivalentes por todo o período de vigência do contrato mantido com a Lilly coma todos os colaboradores do Terceiro/Fornecedor que lidarem com as Informações da Lilly. Os acordos de confidencialidade devem obrigatoriamente incluir, mas não estão limitados a:

a. Obrigações de confidencialidade pós-emprego/contratação.
b. Disposições que regem o uso aceitável de recursos eletrônicos, incluindo, mas não se limitando ao uso de recursos eletrônicos de maneira profissional, legal e ética.

# Padrão de Segurança da Informação (ISS)

Devem existir processos para identificar e coletar ativos (físicos e eletrônicos) de indivíduos ao se desvincularem do Terceiro/Fornecedor ou daqueles que não precisam mais de acesso às Informações.

**6. Acesso às Informações**

O Terceiro/Fornecedor deve possuir, no mínimo, os seguintes controles de ativação de conta em vigor quando tiver acesso à Informações pertencentes ou confiadas pela Lilly ao Terceiro/Fornecedor e/ou que estejam armazenadas fora do ambiente da Lilly e/ou quando o Terceiro/Fornecedor possuir uma conexão de acesso remoto ao ambiente da Lilly:

a. Um processo de aprovação formal para conceder acesso com base em uma necessidade comercial compatível com as funções de trabalho desempenhadas pelo pessoal do Terceiro/Fornecedor, ou seja, privilégios mínimos de acesso à Informação ou nível de acesso necessário, mas nunca maior do que o necessário.
b. Segregação entre solicitação, aprovação e concessão de acesso.
c. As contas de usuário para acesso a sistemas, serviços e aplicativos devem ser atribuídas a usuários individuais e não podem ser compartilhadas.
d. As contas de usuário privilegiado e/ou administrativo devem ser diferentes das contas de usuário padrão e possuir IDs de login de usuário exclusivo. Contas privilegiadas (nível elevado de acesso, que concede poderes dentro de um sistema de computador, os quais são significativamente maiores do que aqueles disponíveis para o usuário comum) devem ser restritas e atribuídas apenas a usuários autorizados.

Os controles de senha devem ser implementados de forma apropriada pelo Terceiros/Fornecedor e devem incluir os seguintes requisitos:

a. Histórico e expiração periódica.
b. As senhas temporárias devem ser comunicadas com segurança e com obrigatoriedade de alteração após o primeiro uso.
c. Alteração imediata de senhas quando houver motivos para acreditar que uma conta foi comprometida.
d. As senhas das contas compartilhadas de sistema, serviço e aplicativo devem ser alteradas quando o pessoal do Terceiro/Fornecedor que tem acesso a senha, deixar o Terceiro/Fornecedor ou mudar para uma posição diferente que não requeira mais o acesso.
e. A identidade do usuário deve ser verificada antes que uma senha seja redefinida.
f. Todas as senhas padrão devem ser alteradas dos valores padrão.
g. Os requisitos de força da senha devem atender ao padrão de segurança comum (por exemplo, ISO, NIST), comprimento e complexidade.

Os seguintes controles de desativação devem estar em vigor pelo Terceiro/Fornecedor:

a. Um processo formal para desativar a tempo as contas das pessoas que se desvincularem do Terceiro/Fornecedor e/ou daqueles que já não têm uma necessidade comercial de ter acesso (por exemplo, no prazo de 24 (vinte e quatro) horas após o desligamento).
b. Processo para garantir uma notificação à Lilly referente a mudanças de pessoal do Terceiro/Fornecedor, dentro do prazo de 24 (vinte e quatro) horas, quando tais empregados têm contas ou têm acesso à Informações ou aos sistemas de informação da Lilly.

Os seguintes controles de acesso devem ser implementados pelo Terceiros/Fornecedor:

a. Revisões periódicas, no mínimo uma vez por ano, de acesso de todos os usuários, contas de sistema, contas de teste e contas genéricas devem ser realizadas e documentadas.
b. As contas de usuário devem ser bloqueadas após um número definido de tentativas de acesso malsucedidas.
c. Contas sem atividade recente (por exemplo, nos últimos 90 (noventa) dias, com exceção daquelas usadas apenas para processamento trimestral, semestral e anual) devem ser desativadas.
d. Os controles de sessão, incluindo bloqueio de conta e tempo limite de sessão, devem estar em vigor.
e. A autenticação multifatorial (MFA) deve estar em vigor para todas as contas privilegiadas e/ou administrativas.
f. O MFA deve estar em vigor para todos os aplicativos voltados para a Internet.
g. O MFA deve estar em vigor para quaisquer métodos de acesso remoto (por exemplo, redes privadas virtuais, protocolos de desktop remoto).

**7. Segurança de rede e sistema**

O Terceiro/Fornecedor deve ter, no mínimo, os seguintes controles de segurança de rede e sistema em vigor quando tiver acesso à Informações pertencentes ou confiadas pela Lilly ao Terceiro/Fornecedor e/ou que estejam armazenadas fora do ambiente da Lilly e/ou quando o Terceiro/Fornecedor possuir uma conexão de acesso remoto ao ambiente da Lilly:

a. Padrões de proteção para sistemas operacionais, aplicativos e dispositivos de rede.
b. Todos os sistemas devem ser corrigidos para o sistema operacional e atualizações de componentes principais após o lançamento do patch relacionado à segurança e avaliação de acordo com os padrões de segurança comuns (por exemplo, ISO, NIST). As vulnerabilidades de alto risco para aplicativos voltados para a Internet deve ser corrigidas o mais rápido possível, não devendo exceder 30 (trinta) dias.
c. Os sistemas devem ser mantidos em níveis para permitir que os patches/service packs de segurança mais recentes sejam aplicados.

Para os controles de segurança de rede:

a. As informações pertencentes ou confiadas pela Lilly ao Terceiro/Fornecedor não devem ser armazenadas em uma zona desmilitarizada (DMZ).
b. As políticas de firewall devem ser implementadas em todas as interfaces de rede que restringem o tráfego de entrada e saída com base na necessidade.
c. Os sistemas de detecção ou prevenção contra invasões devem ser implementados para detectar e responder ao tráfego de rede não autorizado ou malicioso.
d. Se houver um acordo de nível de serviço de disponibilidade em um sistema ou aplicativo entre a Lilly e o Terceiro/Fornecedor, a proteção de negação de acesso distribuída (DDoS) está em vigor.

Controles de segurança de sistemas:

a. Os dispositivos “endpoint” devem ser criptografados e protegidos com uma senha.
b. Os terminais móveis (smartphones, tablets) devem ser protegidos por meio de um sistema de gerenciamento de dispositivos móveis.
c. Os servidores e “endpoints” devem ser protegidos usando proteção contra vírus/malware que são mantidos atualizados.

## 8. Registro e monitoramento

As atividades de registro devem ser documentadas e realizadas de acordo com os padrões de segurança comuns (por exemplo, ISO, NIST). O monitoramento deve identificar minimamente os eventos de segurança cibernética e verificar a eficácia das medidas de proteção.

## 9. Gerenciamento de ameaças e vulnerabilidades

O Terceiro/Fornecedor deve realizar avaliação de vulnerabilidade contínua e processo de correção em tempo hábil para aplicativos, sistema operacional e outros componentes de infraestrutura. Além disso, os serviços e processos devem ser projetados para identificar, avaliar, mitigar e proteger as Informações contra ameaças e vulnerabilidades de segurança novas e existentes, incluindo vírus, boots e outros códigos maliciosos.

O Terceiro/Fornecedor deve possuir os seguintes controles em vigor:

a. Testes anuais de penetração independentes em suas redes e aplicativos que lidam com as Informações.

b. Varreduras de vulnerabilidade trimestrais devem ser realizadas em suas plataformas e redes que lidam com as Informações para garantir o alinhamento com os padrões de segurança comuns especificamente relacionados à proteção do sistema.
c. Um programa de remediação baseado em risco para resolver em tempo hábil descobertas de testes de penetração, varreduras de vulnerabilidade e avaliações de conformidade.
d. Conforme necessário, o Terceiro/Fornecedor trabalhará para acomodar as solicitações da Lilly para realização de teste de penetração de rede.

**10. Gerenciamento de Mudança**

O Terceiro/Fornecedor deve implementar uma política de controle de mudança documentada que deverá incluir:

a. Requisitos de aprovação, classificação, teste e plano de retorno.
b. Segregação de funções entre solicitação, aprovação e implementação.
c. Gestão e revisão de mudanças de emergência dentro de um período fixo (por exemplo, 24 (vinte e quatro) horas).

**11. Gestão de ativos**

O Terceiro/Fornecedor deve manter um inventário de ativos, incluindo sistema/dispositivo e ativos de software quando tiver acesso à Informações pertencentes ou confiadas pela Lilly ao Terceiro/Fornecedor e/ou que estejam armazenadas fora do ambiente da Lilly e/ou quando o Terceiro/Fornecedor possuir uma conexão de acesso remoto ao ambiente da Lilly.

O Terceiro/Fornecedor deve ter controles de descarte de ativos em vigor para garantir que as Informações (cópia impressa e eletrônica) sejam descartadas de acordo com os padrões de segurança comuns (por exemplo, ISO, NIST) e requisitos legais aplicáveis quando não forem mais necessários, além de manter evidências documentadas de descarte adequado.

**12. Tratamento de Informações**

O Terceiro/Fornecedor deve garantir a separação física ou lógica das Informações de outras informações da Lilly, de outros clientes e das próprias informações do Terceiro/Fornecedor sempre que o Terceiro/Fornecedor tiver acesso à Informações pertencentes ou confiadas pela Lilly ao Terceiro/Fornecedor e/ou que estejam armazenadas fora do ambiente da Lilly e/ou quando o Terceiro/Fornecedor possuir uma conexão de acesso remoto ao ambiente da Lilly.

Além disso, o Terceiro/Fornecedor deve ser capaz de produzir uma descrição do fluxo das Informações em seus ambientes.

Trocas eletrônicas de informações entre a Lilly e o terceiro/fornecedor (incluindo e-mail, transferência de arquivos, conectividade remota, etc.) devem ser protegidas usando serviços mutuamente acordados por escrito.

Processos e ferramentas devem ser usados para prevenir, detectar e responder à perda das Informações.
As informações não devem ser armazenadas ou transferidas usando dispositivos de armazenamento removíveis sem aprovação documentada da Lilly (obtida por meio do processo de solicitação de armazenamento removível da Lilly). Se tais dispositivos forem utilizados, todas as informações armazenadas no dispositivo devem ser criptografadas.

## 13. Encriptação

A encriptação é necessária para as Informações em trânsito quando o Terceiro/Fornecedor tiver acesso à Informações pertencentes ou confiadas pela Lilly ao Terceiro/Fornecedor e/ou que estejam armazenadas fora do ambiente da Lilly e/ou quando o Terceiro/Fornecedor possuir uma conexão de acesso remoto ao ambiente da Lilly.

As chaves de criptografia pertencentes ou gerenciadas pelo Terceiro/Fornecedor devem ser armazenadas em um local seguro separado do local onde as Informações são armazenadas com acesso gerenciado, juntamente com capacidade de recuperação de chave demonstrada.

Os procedimentos e práticas de criptografia devem atender aos padrões de segurança comuns atuais (por exemplo, ISO, NIST).

## 14. Segurança física

Os controles físicos e de processos devem ser estabelecidos e aplicados para proteger as cópias impressas e os sistemas de informação (por exemplo, hardware, software, documentação e dados) quando o Terceiro/Fornecedor tiver acesso à Informações pertencentes ou confiadas pela Lilly ao Terceiro/Fornecedor e/ou que estejam armazenadas fora do ambiente da Lilly e/ou quando o Terceiro/Fornecedor possuir uma conexão de acesso remoto ao ambiente da Lilly.

Os Data Centers devem estar sob controle físico, com acesso formalmente gerenciado com base nas necessidades de negócio do Terceiro/Fornecedor. Os Data Centers devem ter controles ambientais (temperatura, umidade, backup de energia) para evitar interrupções ou perdas de Informações.

Uma avaliação anual independente de segurança física das instalações deve ser exigida caso o Terceiro/Fornecedor transmita, armazene e/ou processe Informações.

**15. Resiliência/Continuidade de Negócios/Backup e Recuperação de Informações**

Além de quaisquer requisitos previstos em um contrato firmado entre a Lilly e o Terceiro/Fornecedor para continuidade de negócios e recuperação de desastres, em conformidade com os requisitos contratuais de negócios e criticidade das Informações, o Terceiro/Fornecedor deve garantir que os seguintes controles estejam em vigor.

a) O poder redundante e a capacidade de alimentação e processamento devem existir dentro da instalação de processamento de dados primários.
b) Garantir que um local de processamento alternativo esteja disponível para continuar os processos de negócios e recuperar a funcionalidade da Lilly dentro da janela de tempo especificada em contrato, se aplicável.
c) Testes de resiliência anuais para demonstrar continuidade de negócios e capacidade de recuperação eficazes devem ser implementados.
d) Os sistemas e dados aplicáveis devem ser submetidos a backup regulares com base na criticidade. A viabilidade dos backups deve ser testada periodicamente.
e) As fitas de backup e/ou transmissões devem ser adequadamente protegidas e segregadas do armazenamento primário.

**16. Retenção e destruição de registros**

O Terceiro/Fornecedor deve reter as Informações apenas pelo tempo especificado no contrato firmado com a Lilly, exceto se um período de retenção mais longo seja exigido por leis ou regulamentos aplicáveis.
Ao fim do contrato com a Lilly, por qualquer motivo, o Terceiro/Fornecedor se obrigada a devolver, excluir ou destruir com segurança as Informações, conforme instruções previstas em contrato, quando aplicável ou fornecidas pela Lilly, exceto as informações em que o Terceiro/Fornecedor, pode reter e fazer uma cópia, em seus arquivos conforme exigível pela lei aplicável.

Mediante solicitação da Lilly, o Terceiro/Fornecedor deve emitir certificado de comprovação de que as Informações foram destruídas conforme as instruções da Lilly.

# Padrão de Segurança da Informação (ISS)

## 17. Resposta, gerenciamento e relatórios de incidentes de segurança da informação

O Terceiro/Fornecedor deve possuir procedimentos de gerenciamento e resposta de incidentes de segurança (por exemplo, exposição, violação, roubo, etc.) que permitam a detecção, investigação, resposta, mitigação e notificação razoáveis de eventos que envolvam uma ameaça à confidencialidade, integridade e/ou disponibilidade das Informações sempre que o Terceiro/Fornecedor tiver acesso à Informações pertencentes ou confiadas pela Lilly ao Terceiro/Fornecedor e/ou que estejam armazenadas fora do ambiente da Lilly e/ou quando o Terceiro/Fornecedor possuir uma conexão de acesso remoto ao ambiente da Lilly. Os procedimentos de gerenciamento e resposta a incidentes devem ser documentados, testados e revisados pelo menos uma vez por ano. Lilly terá a opção de revisar tais procedimentos mediante solicitação.

O Terceiro/Fornecedor deve notificar a Lilly imediatamente, mas não depois do prazo de 48 (quarenta e oito) horas, contados do evento, sobre incidentes de segurança suspeitos ou conhecidos que tenham impacto potencial nas Informações. Além disso, o Terceiro/Fornecedor deve ter um processo documentado, com contatos definidos da Lilly e do Terceiro/Fornecedor, para garantir a conformidade com este requisito de notificação.

O Terceiro/Fornecedor deve cooperar totalmente com a Lilly para entender a situação, a causa raiz e determinar a correção necessária no caso de um incidente de segurança real ou suspeito.

## 18. Gestão de Subcontratados

Este Padrão de Segurança da Informação se aplica a todos os subcontratados utilizados pelo Terceiro/Fornecedor que lidam com Informações pertencentes ou confiadas pela Lilly que estejam armazenadas fora do ambiente da Lilly e/ou quando o Terceiro/Fornecedor possuir uma conexão de acesso remoto ao ambiente da Lilly. É responsabilidade do Terceiro/Fornecedor garantir que o Padrão de Segurança da Informação seja comunicado e cumprido por cada subcontratado que tenha acesso as Informações. Para evitar dúvidas, os subcontratados incluem, mas não se limitam a, reprografia de terceiros/fornecedores, terceiros/fornecedores de armazenamento externo, desenvolvedores de software, instalações de hospedagem em nuvem e instalações de data center.

Contratos formais entre Terceiros/Fornecedor e subcontratados devem ser firmados, descrevendo os controles a serem fornecidos, incluindo controles para manter a confidencialidade, disponibilidade e integridade das Informações.

Avaliações iniciais e contínuas devem ser conduzidas pelo Terceiro/Fornecedor a fim de garantir que os subcontratados estejam aderindo ao Padrão de Segurança da Informação e que os incidentes e problemas de segurança sejam gerenciados de forma adequada.

O Terceiro/Fornecedor deve informar a Lilly e obter aprovação por escrito antes de autorizar o acesso às Informações da Lilly por subcontratados.

**19. Direitos de análise de segurança da informação**

O Terceiro/Fornecedor deve permitir que a Lilly e seus agentes, auditores (internos e/ou externos) e/ou quaisquer outros representantes inspecionem, auditem, examinem e revisem as instalações, livros, sistemas, registros, listas de acesso, dados, práticas e procedimentos do Terceiro/Fornecedor e de quaisquer subcontratados que o Terceiro/Fornecedor possa usar, para verificar a integridade das Informações e monitorar o cumprimento desta Norma de Segurança da Informação.

**20. Ciclo de vida de desenvolvimento do sistema**

Os requisitos abaixo serão aplicáveis apenas no caso de desenvolvimento pelo Terceiro/Fornecedor de software ou aplicativos para a Lilly.

Metodologia de Engenharia de Desenvolvimento de Software:

a. Uma metodologia de desenvolvimento de sistemas definida deve ser formalmente implementada com políticas, procedimentos e padrões comunicados e seguidos e devem estar alinhados aos padrões da indústria. Padrões de programação devem ser desenvolvidos e comunicado aos membros relevantes da força de trabalho. Os padrões incluem arquitetura e especificações de design, revisão de lógica de negócios, adoção de algoritmos e bibliotecas seguras, remoção de teste código e a correção de falhas de segurança comuns (por exemplo, as dez principais vulnerabilidades do OWASP).
b. As revisões de código devem ser realizadas para confirmar a adesão aos padrões de programação anteriores.
c. O uso de dados de produção em ambientes de não produção deve ser feito somente quando necessário e da mesma forma os controles de segurança devem estar em vigor no ambiente de produção ou nas informações de produção usado no teste deve ser suficientemente ofuscado.
d. Software que está disponível em domínio público (por exemplo, software de código aberto, shareware, freeware), se usado, deve ser devidamente examinado para risco potencial, incluindo risco legal potencial (por exemplo, violação de direitos autorais).
e. Software que está disponível em domínio público (por exemplo, software de código aberto, shareware, freeware), se usado, deve incluir controles para garantir que a introdução deste tipo de software não terá um impacto negativo (por exemplo, vírus, cavalo de tróia, violações de segurança como "backdoor").

f. O código-fonte deve ser mantido em uma ferramenta de controle de versão não pública aceita pela indústria, com controles rígidos relacionado à verificação do código-fonte. O Terceiro/Fornecedor deve ter sistemas de monitoramento que monitoram mudanças de código de ambiente.
g. Gerenciar o ciclo de vida de segurança de todos os softwares desenvolvidos e adquiridos internamente

Liberação de Código:

a. O Terceiro/Fornecedor deve buscar a melhoria contínua em seu modelo de desenvolvimento escolhido.
b. O Terceiro/Fornecedor deve ter uma política/procedimento formal de gestão de mudança/liberação para o planejamento de atualizações de software que demonstrem que as versões são planejadas, gerenciadas, testadas, aprovadas e comunicada de forma apropriada, a Lilly será notificada com antecedência sobre as mudanças programadas.
c. Os ciclos de gerenciamento de mudanças/liberações começam com a definição dos requisitos. Impacto, feedback e necessidade da Lilly devem ser devidamente fatorados nos requisitos de liberações planejadas.
d. O teste de regressão deve ser executado durante cada ciclo de liberação. O teste deve ser realizado em vários níveis. (por exemplo, unidade, integração e sistema, usuário). O teste do usuário deve ser baseado em planos de teste formais, realizados por partes independentes para aqueles que projetam e desenvolvem o sistema.
e. As aprovações formais devem ser capturadas em cada estágio do ciclo de vida de desenvolvimento (Requisitos, Design, Teste, Aceitação do usuário, implementação da produção, etc.). Quando as aprovações são capturadas, deve ficar claro quem está aprovando, a data em que estão aprovando e o que estão aprovando.
f. Versões e patches devem ser fornecidos com instruções suficientes para implantação e/ou uso. Isso inclui aquelas soluções em que a Lilly recebe o lançamento ou patch para se aplicar, bem como aquelas em que a Lilly está sendo notificada sobre uma mudança que o Terceiro/Fornecedor aplicou em um ambiente da Lilly.
g. Os projetos de sistema devem ser criados formalmente para auxiliar na tradução dos requisitos para o código.

Alterações provisórias/correções de bugs:

a. Um procedimento formal para implementar mudanças de emergência/correção de bug, incluindo aquelas para lidar com vulnerabilidades de segurança, deve estar em vigor para confirmar que essas mudanças podem ser feitas em tempo hábil, mas de maneira controlada.
b. Um processo formal deve estar em vigor para comunicar bugs ou defeitos conhecidos à Lilly.
c. As alterações de correção de bug devem ser testadas formalmente e demonstrar documentação e aprovações adequadas. A aprovação deve ser concedida por alguém que não seja o indivíduo que está fazendo a mudança.