REGRAS DE NEGÓCIOS PARA MANUSEIO SEGURO DE INFORMAÇÕES

Objetivo: mensagens importantes para lidar com informações da Lilly ou em nome dela, doravante denominadas Informações.

Qual é a importância disso?

- Sua organização e sua força de trabalho são colaboradores valiosos para a Lilly, e as ações que vocês realizam compõem parte da primeira e melhor linha de defesa contra o comprometimento das Informações.
- Proteger as Informações é essencial para a Lilly e os pacientes que atendemos.

As mensagens importantes abaixo, que são fornecidas a partir das práticas recomendadas do setor, como a Estrutura de segurança cibernética do NIST, devem ser incorporadas às práticas atuais para continuar reduzindo riscos ao lidar com as Informações.

No geral:

- Evite fazer cópias eletrônicas ou impressas duplicadas de documentos que contenham Informações, a menos que seja absolutamente necessário.

Armazenamento eletrônico de dados:

- Os arquivos eletrônicos que incluem Informações devem ser armazenados de forma segura. Dispositivos de armazenamento removíveis, como discos rígidos externos e USBs, não podem ser usados sem a aprovação da Lilly.
    - O Princípio de privilégios mínimos deve ser aplicado para conceder acesso aos arquivos (ou seja, o acesso às Informações só deve ser concedido àqueles que precisam sabê-las, não mais do que o exigido e apenas pelo tempo necessário). O acesso deve ser analisado de acordo com o nível de confidencialidade. Isso vale para locais de armazenamento que você gerencia, bem como aqueles gerenciados por seus subcontratados.
    - A desativação oportuna do acesso deve ocorrer após uma saída da empresa ou quando os indivíduos não tiverem mais a necessidade comercial de acessar as Informações.
- As Informações NÃO devem ser armazenadas nos seguintes locais sem a aprovação da Lilly:
    - Dispositivos pessoais de funcionários, como laptops, iPad etc.
    - Serviços ou sites de armazenamento externo.

Transferência de dados eletrônicos:

- Os arquivos eletrônicos que incluem Informações devem ser transferidos de forma segura. Consulte seu contato da Lilly para estabelecer o método de preferência para transferência de Informações. Dispositivos de armazenamento removíveis, como discos rígidos externos, CDs/DVDs e USBs, não podem ser usados sem a aprovação da Lilly.
- As Informações NÃO devem ser transferidas por meio de:
    - E-mail não seguro (a menos que o nível de confidencialidade não justifique).
    - Dispositivos de armazenamento externo, como disco rígido externo ou USB (sem aprovação da Lilly).
    - E-mail pessoal.

Teleconferências/reuniões on-line:

- Use os serviços de reunião aprovados pela Lilly para agendar e realizar reuniões sobre negócios da empresa. Consulte seu contato da Lilly se tiver perguntas relacionadas a teleconferências/reuniões on-line.
- Esteja ciente de seus arredores e seja cauteloso ao discutir Informações.

Segurança física:

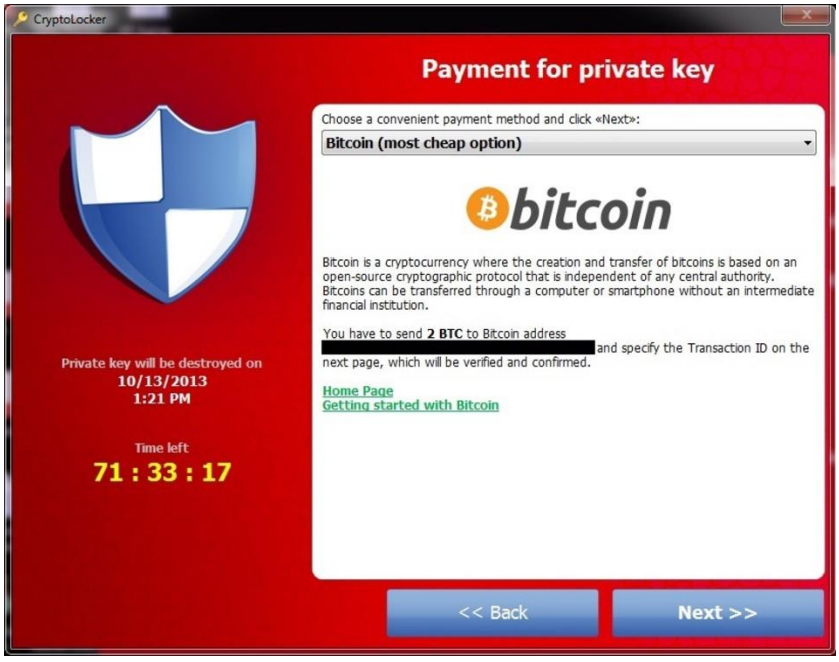
- Mantenha um espaço de trabalho seguro:
    - Bloqueie o acesso aos seus dispositivos SEMPRE que se afastar deles.
    - Coloque os dispositivos em um armário com fechadura, tranque-os com cadeado ou leve-os com você ao se ausentar, viajar a negócios ou sair de férias.
    - Deixe a mesa, armários e gabinetes no escritório trancados ao se ausentar, viajar a negócios ou sair de férias.
    - Não deixe cópias impressas nas impressoras.
    - Descarte Informações confidencialmente (por exemplo, com fragmentadora).

Mensagem instantânea e texto:

- Utilize uma ferramenta aprovada pela Lilly para mensagens instantâneas e de texto para os negócios da empresa. Consulte seu contato da Lilly se tiver dúvidas relacionadas a mensagens instantâneas ou de texto.

Relatório de incidentes de segurança da informação:

- Relate incidentes ao seu contato da Lilly em tempo hábil. A lista abaixo traz exemplos, mas não é exaustiva:
    - E-mail com Informações que tenha sido enviado acidentalmente a um destinatário indesejado.
    - Laptop, disco rígido ou dispositivo de armazenamento removível perdido ou roubado que contenha Informações.
    - Alerta recebido de um subcontratado com acesso a Informações sobre um incidente.
    - Recebimento de ransomware, um tipo de software malicioso projetado para bloquear o acesso ao dispositivo até que uma quantia seja paga. Veja o exemplo abaixo. Realize estas etapas imediatamente para reduzir o risco:
        - Desconecte o cabo de rede ou desative o adaptador sem fio.
        - Coloque o dispositivo no modo de hibernação.



Esteja a tento à engenharia social *(por exemplo, phishing, vishing, smishing)*:

- Engenharia social é o uso de fraude para convencer pessoas a divulgar informações confidenciais ou pessoais que possam ser usadas para fins fraudulentos. Os golpistas se disfarçam de uma fonte confiável para tentar roubar identidades ou capturar Informações, como senhas, dados bancários e números de cartão de crédito etc.

- **Phishing** (por e-mail)
  - Uma tentativa de phishing é uma mensagem inesperada, e estas são algumas das características:
    - Um apelo à ação chamativo (por exemplo, seu pagamento com cartão de crédito está atrasado).
    - Uma referência ao tempo (por exemplo, algo deve ser entregue em dois dias).
    - Uma consequência (por exemplo, resolva este problema, senão algo ruim acontecerá com você).
    - Erros gramaticais ou ortográficos.
    - E sempre há algum item para "clicar", como um link ou anexo
  - Se você clicar em um anexo ou link desconhecido em um e-mail, seu computador e toda a rede podem ser comprometidos.

- **Vishing** (ligações ou mensagens de voz)
  - Uma tentativa de vishing (phishing de voz) é uma chamada telefônica inesperada que:
    - Solicita confirmação de Informações ou apenas Informações.
    - Pode ser aplicada com um ataque de phishing.
- **Smishing** (mensagens de texto por SMS)
  - Uma tentativa de smishing é uma mensagem inesperada que:
    - Solicita confirmação de Informações ou apenas Informações.
    - Pode ser aplicada com um ataque de phishing.
    - Normalmente tem algo para "clicar", como um link ou anexo.

- **Se você tiver um endereço de e-mail da Lilly**, você participará do programa formal de instrução sobre phishing.
  - As pessoas que têm o hábito de clicar sem prestar atenção serão relatados ao terceiro e poderão passar por treinamento. Consulte seu contato da Lilly se tiver dúvidas sobre o programa formal de instrução sobre phishing.
  - Se você estiver usando uma conta de e-mail o365 da Lilly, denuncie e-mails suspeitos por meio do botão "Report Phishing" (Denunciar phishing) na faixa "Home" (Página inicial) do Outlook.

  - Se você estiver conectado à rede interna da Lilly via VPN ou virtual.lilly.com, denuncie mensagens suspeitas por cyber@lilly.com

- **Faça uma pausa e inspecione. Use sua intuição:**
  - Se um e-mail parecer suspeito, analise a mensagem com atenção.
  - Não clique em links nem abra anexos pelos quais você não estava esperando.
  - Se você não tiver um endereço de e-mail da Lilly e clicar em um link ou abrir um anexo de uma mensagem que acredita ser suspeita, denuncie por meio do processo do seu empregador.

Se você tiver dúvidas ou preocupações:

- Consulte seu contato da Lilly se tiver dúvidas ou preocupações relacionadas aos itens discutidos acima.
- Estas informações também estão disponíveis no Supplier Portal (Portal do fornecedor) em Operating Responsibility (Responsabilidade operacional) nos Supplier Resources (Recursos do fornecedor).