O DESAFIO DA LGPD NO CONTEXTO DE ADERÊNCIA E MATERIALIZAÇÃO DAS NORMAS E REGRAS

Uma abordagem para atendimento e blindagem das instituições

Dayna Maria Bortoluzzi
dayna@sef.sc.gov.br

SUMÁRIO EXECUTIVO

- O DESAFIO
- Governança da Privacidade SEFAZ-RE
- A Implementação da POSIC adequada a LGPD em SC
- A construção de um ambiente de proteção
- Próximos passos e recomendações finais

O DESAFIO

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 09/07/2019 | Edição: 130 | Seção: 1 | Página: 1

Órgão: Atos do Poder Legislativo

LEI Nº 13.853, DE 8 DE JULHO DE 2019

Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

O PRESIDENTE DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º A ementa da Lei nº 13.709, de 14 de agosto de 2018, passa a vigorar com a seguinte redação:

"Lei Geral de Proteção de Dados Pessoais (LGPD)."

PREMISSAS

A LGPD se aplica a qualquer organização que utilize dados pessoais inclusive por meios digitais.

(coleta, armazenamento, processamento, exclusão, etc.)

- **Direitos** de privacidade pessoal
- **Aumento** do dever de proteger dados
- **Relatório** de violação obrigatório
- **Penalidades** por descumprimento

COMO FAZER?

1) Identificar e priorizar processos de negócio que precisam de proteção (Governança da Privacidade)
2) Definir ou adaptar a Política de Segurança da Informação
3) Criar um Comitê de Segurança da Informação
   - Pode instituir grupos de trabalho ou câmaras técnicas;
   - Pode estabelecer sua forma de funcionamento e suas competências.
4) Classificar as informações
5) Implantar mecanismos que permitam que a POSIC seja consolidada conforme sua definição
   - Definir um setor(es) responsável(eis) pelo relatório de incidentes

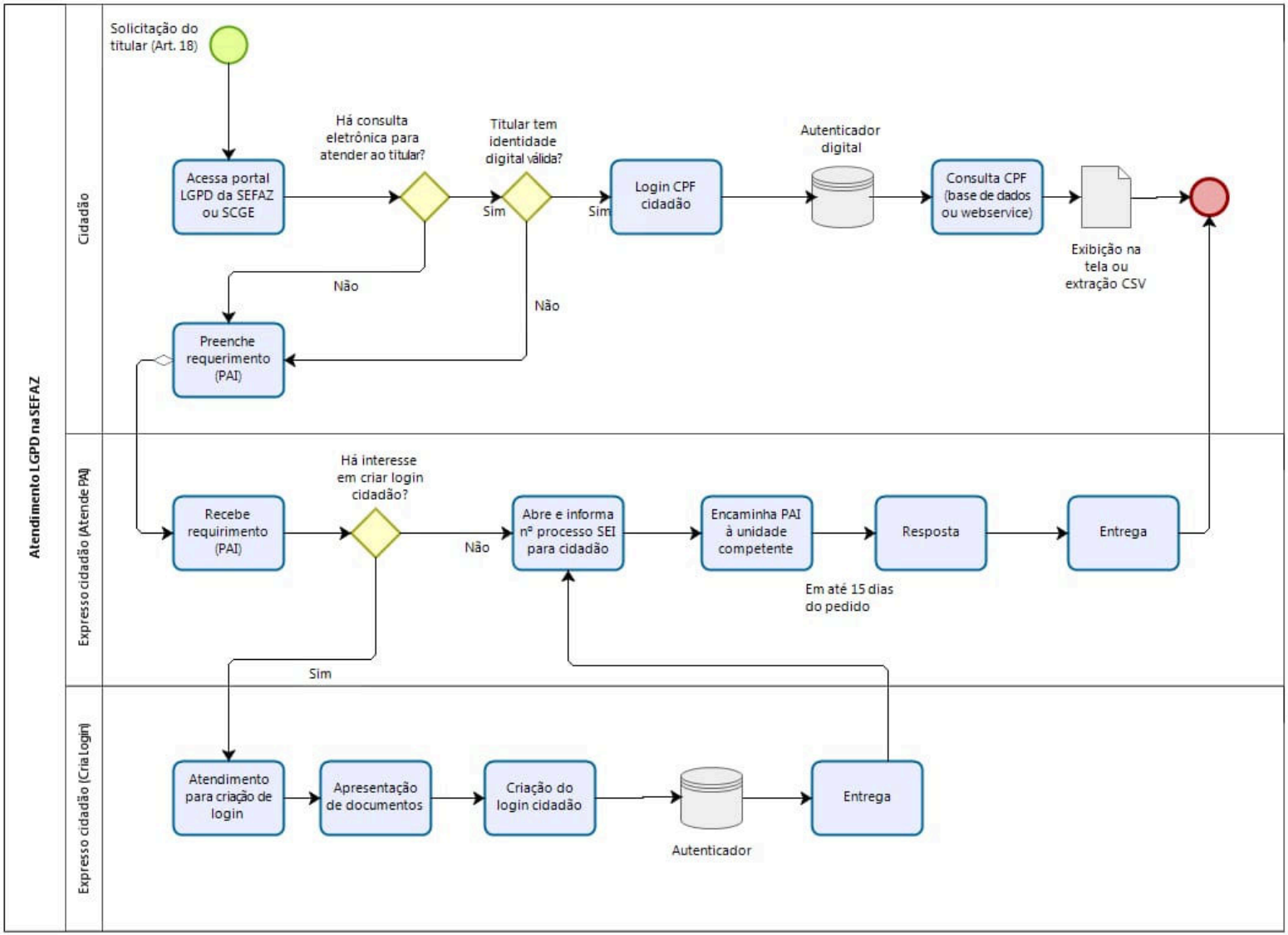
GABA – GABINETE DO SECRETÁRIO ADJUNTO
DIAT – DIRETORIA DA ADMINISTRAÇÃO TRIBUTÁRIA
DCIF – DIRETORIA DE CONTABILIDADE E INFORMAÇÕES FISCAIS

GOVERNANÇA DA PRIVACIDADE

- Identificar os processos de negócio e os ativos de sustentação (aplicações e dados)
  - Como? Entrevistas com área de negócio e/Ou TI
  - Ex: gestão da arrecadação/sistema xpto/relação de dados pessoais utilizados
  - Organizar resultados em planilhas ou sistemas específicos de governança de privacidade
- Analisar lacunas da proteção atual à luz da LGPD
  - Como? Cotejar as exigências legais com os controles existentes
  - Exemplo: Art. 46 exige controle contra acesso indevido (vazamento)
  - Fato: sistema xpto não é monitorado p/ vazamento nem há procedimento contenção
- Avaliar riscos das lacunas, e classificá-las por nota (gestão de riscos)
  - Sistema xpto tem risco alto, e vazamento pode gerar ação cível de R$ 1 milhão
- Para cada risco, um plano de ação adequado
  - Mitigar o risco do sistema xpto, através da aquisição de monitoramento com alarmes e contenção de vazamentos

Governança da Privacidade é um processo de negócio

- É um processo de controle da alta gestão
  - É permanente, tem indicadores para análise crítica.
  - Responsabilidade do controlador, delegada ao DPO e sua equipe
- DPO (Data Protection Officer) define objetivos e metas da governança, que são submetidos à gestão de risco e conformidade
  - Ex: 100% processos de arrecadação em conformidade com LGPD até 2021.
- A Gestão de riscos informa quais processos de negócio são prioritários para ajustes
- A Conformidade audita processos de negócio, avaliados pelo DPO na análise crítica
- Relatórios de Conformidade podem suscitar novos objetivos e metas (PDCA)


Atendimento LGPD na SEFAZ
Cidadão
Expresso cidadão (Atende PAI)
Expresso cidadão (Cria Login)
Solicitação do titular (Art. 18)
Acessa portal LGPD da SEFAZ ou SCGE
Há consulta eletrônica para atender ao titular?
Sim
Não
Titular tem identidade digital válida?
Sim
Não
Login CPF cidadão
Autenticador digital
Consulta CPF (base de dados ou webservice)
Exibição na tela ou extração CSV
Preenche requerimento (PAI)
Recebe requirimento (PAI)
Há interesse em criar login cidadão?
Não
Sim
Abre e informa nº processo SEI para cidadão
Encaminha PAI à unidade competente
Em até 15 dias do pedido
Resposta
Entrega
Atendimento para criação de login
Apresentação de documentos
Criação do login cidadão
Autenticador
Entrega

POSIC – Política de Segurança da Informação e Comunicação

- Trata do uso e compartilhamento dos dados, informações e documentos da SEF

- É aplicada a todos os colaboradores que acessam e/ou possuem conta com autenticação na rede da SEF (servidores públicos, terceirizados, consultores, fornecedores ou estagiários).
  - Obrigatória assinatura de Termo de Confidencialidade
  - Obrigatório o conhecimento e anuência da Política de Privacidade e Termos de Uso do SAT, para quem atua na equipe de desenvolvimento.

POSIC - Tratamento da Informação

- **Toda informação** criada, adquirida ou custodiada no exercícios de sua atividade é de **propriedade** da SEF
- É proibido acesso, guarda ou encaminhamento de material discriminatório, obsceno, ilegal, não ético por quaisquer meio disponibilizado pela tecnologia da informação e comunicação da SEF
- **Os ativos devem ser protegidos de forma preventiva**
- As **informações** devem ser **classificadas** de acordo com o grau de sigilo
- As informações produzidas ou custodiadas pela SEF devem ser descartadas de acordo com seu nível de classificação.
- A **destruição de dados sigilosos** deve ser feita por método que sobrescreva as informações armazenadas, quando não possível deve ser feita a destruição física do equipamento.

POSIC – Tratamento de Incidentes

- A Gerência de Tecnologia da Informação é responsável por analisar e responder notificações e atividades relacionadas a incidentes de segurança
- Criar e manter registros e procedimentos, como trilhas de auditoria, que possibilitem o rastreamento e controle de acessos aos sistemas
- Verificação da conformidade:
  - Dos contratos e acordos de cooperação técnica;
  - Da análise de documentos, registros (logs), código fonte, entrevistas e testes de invasão;
  - Os resultados serão apresentados em Relatório de Avaliação da Conformidade

SÃO ATRIBUIÇÕES:

- **Do Comitê de Segurança da Informação**
  - Atualizar a POSIC
  - Propor, analisar e aprovar normas complementares relativas a SIC
  - Tratar dos assuntos de segurança da informação e assessorar o Gabinete
- **Da Gerência de Tecnologia**
  - Planejar, coordenar, supervisionar, executar e controlar a execução das atividades de TIC
  - Elaborar, implementar e atualizar normas internas em conformidade com a POSIC
  - Coordenar a manutenção dos registros, fazer o rastreamento e verificar o acesso a todas as redes computacionais da SEF;
  - Agir proativamente para evitar incidentes de segurança;
  - Coordenar ações reativas ao tratamento de incidentes.

(cont ...)

SÃO ATRIBUIÇÕES:

- **Da Gerencia de Sistemas e Informações Tributárias**
- Planejar, coordenar, supervisionar, executar e controlar a execução das atividades de TIC
- Coordenar ações reativas que incluem recebimento de notificações de incidentes relativos aos Sistemas de Adm. Tributária
- Coordenar ações que visam garantir o intercâmbio de informação sigilosa
  - Entregar informações pessoalmente à autoridade solicitante;
  - Coordenar ações para coibir a divulgação de informações custodiadas pela SEF
  - Coordenar ações para tratar incidentes relativos às falhas de segurança dos sistemas

O que mudou na POSIC após a LGPD

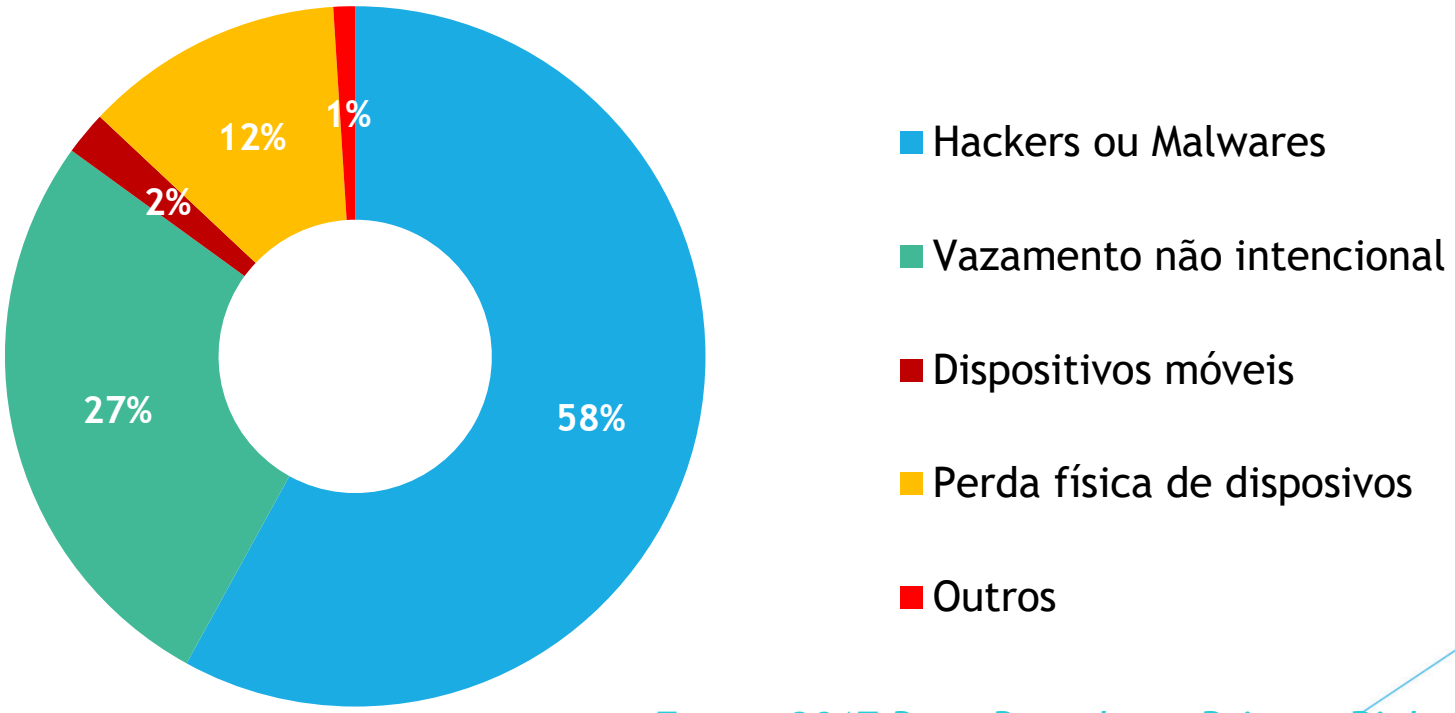
- A implementação ou contratação de computação em nuvem no âmbito da SEF deve ser definida em norma específica;
- A cifração e a decifração de informações classificadas em qualquer grau de sigilo devem utilizar recurso criptográfico;
- Qualquer sistema utilizado na SEF e que contenham tabelas com senhas, deverão ter estas tabelas armazenadas criptografadas.

Ações imediatas

- Aquisição de Licenças para BD com funcionalidades de segurança;
- Implantar uma estrutura de defesa cibernética

O DESAFIO DA PROTEÇÃO DOS DADOS

Como as empresas perdem dados?

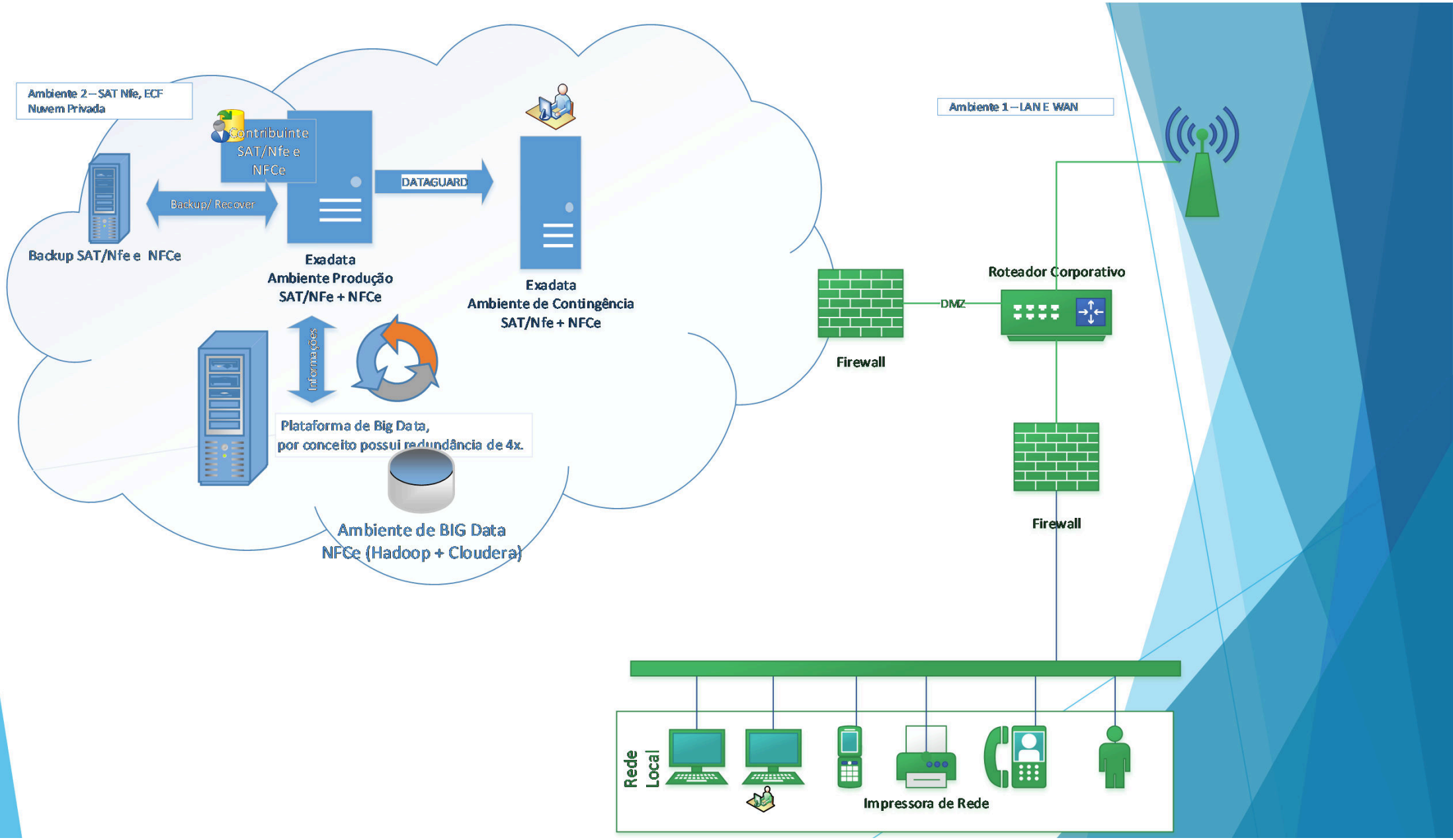


Fonte: 2017 Data Breaches – Privacy Rights Clearinghouse

CAPÍTULO VII
DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I
Da Segurança e do Sigilo de Dados

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.


Ambiente 2 – SAT Nfe, ECF
Nuvem Privada
Contribuinte SAT/Nfe e NFCe
Backup/ Recover
DATAGUARD
Backup SAT/Nfe e NFCe
Exadata
Ambiente Produção
SAT/NFe + NFCe
Exadata
Ambiente de Contingência
SAT/Nfe + NFCe
Informações
Plataforma de Big Data,
por conceito possui redundância de 4x.
Ambiente de BIG Data
NFCe (Hadoop + Cloudera)
Ambiente 1 – LAN E WAN
Roteador Corporativo
DMZ
Firewall
Firewall
Rede Local
Impressora de Rede

A infraestrutura de defesa

- BANCO DE DADOS (Oracle Options)
  - Advanced Security: criptografia dos dados e a redação de dados confidenciais exibidos pelos aplicativos
  - Data Vault: protege os dados do aplicativo contra acesso não autorizado e implementa a separação de tarefas entre administradores de BD e proprietários dos dados para atender requisitos regulatórios e de privacidade
  - Label Security: permite a consolidação dos dados em conjuntos semelhantes de dados confidenciais mas com requisitos de acesso diferentes no mesmo banco de dados
  - Data Masking and Subsetting Pack: mascara e agrupa dados de produção confidenciais, permitindo que os dados sejam compartilhados com segurança em ambientes que não sejam de produção

A infraestrutura de defesa (cont.)

- PROTEÇÃO DO MEIO DE ACESSO
  - Estações de Trabalho, dispositivos móveis, ambiente de armazenamento (físico ou nuvem)
  - Controle de acesso à WEB, controle de aplicativos, periféricos
  - Controle de vazamento de dados, proteção contra ameaças virtuais e códigos maliciosos
  - Impedir que usuários executem ou instalem aplicações que possam afetar a produtividade da rede
  - Ter capacidade de bloquear a execução de aplicativos que está em armazenamento externo à LAN
  - Gerenciar dispositivos externos (PEN Drives, storages, CD, DVD e celulares)

A infraestrutura de defesa(cont.)

- PROTEÇÃO SOBRE QUEM ACESSA OS DADOS
  - Levantamento de credenciais de acesso
    - Âmbito corporativo e terceiros (Prestadores de serviço)
  - Gerenciamento das credenciais utilizadas
    - Rotação das credenciais de acesso, inclusive dos sistemas
    - Permitir a entrega de sessão autenticada sem que o usuários tenha contato com a senha real
  - Monitoramento do uso das credenciais utilizadas
    - Gestão sobre as permissões, horários e atividades permitidas
  - Auditoria das credenciais
    - Registro e monitoramento com gravação de sessão para permitir a investigação de incidentes de segurança

A infraestrutura de defesa (cont.)

- RASTREABILIDADE
  - Monitoramento contínuo do tráfego da LAN de forma a não ser utilizado em atividades não permitidas
  - Registro sobre os acessos internos ou à nuvem
  - Análise comportamental dos acessos
  - Auditoria sobre os acessos
- ANALISE DO CÓDIGO FONTE DOS APLICATIVOS

Recomendações Finais

- Implementar a formalização dos processos
  - Fazer o levantamento dos riscos operacionais dos sistemas
    - Temos como modelo às planilhas e a metodologia da SEFAZ-RE
  - Adequar a Política de Segurança do Órgão às novas demandas de proteção de dados
  - Formalizar a politica de segurança da informação
    - Temos como modelo a Portaria da SEFAZ-SC

- Focar em paralelo na execução
  - Testar ferramentas para assegurar a LGPD
  - Divulgar os resultados obtidos na COGEF TI