RIBEIRO DE ANDRADE
advogados

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
Diretrizes e Normas Administrativas

RENATO MORAES BICALHO DE LANA

Assinado digitalmente por RENATO MORAES BICALHO DE LANA
DN: C=BR, O=ICP-Brasil, OU=AC OAB, OU=38733101000144, OU=Presencial, OU=Assinatura Tipo A3, OU=ADVOGADO, CN=RENATO MORAES BICALHO DE LANA
Razão: Eu sou o autor deste documento
Localização: sua localização de assinatura aqui
Data: 2021.11.22 17:37:07-03'00'
Foxit PDF Reader Versão: 11.0.0

Documento revisado e aprovado pela Alta Administração – 1ª versão
Documento revisado e aprovado pela Alta Administração – 2ª versão

Belo Horizonte, novembro de 2021

www.RIBEIRODEANDRADE.adv.br randradeadv@ribeirodeandrade.adv.br
Tel: (31) 3025-3464
Fax: (31) 3275-1656
RA advogados

1. INTRODUÇÃO

A presente Política de Segurança da Informação (“PSI”) é baseada nas recomendações da norma ABNT NBR ISO/IEC 27002:2013, documento de orientação para organizações implementarem controles de segurança da informação comumente aceitos.

“O valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos.”. (ABNT NBR ISO/IEC 27002:2013)

O Ribeiro de Andrade (“Escritório”) entende a informação como ativo de grande valor, sendo que, para protege-la, segue uma série de normas e diretrizes, partindo das três principais fontes de requisitos da segurança da informação:

a) Avaliação de riscos;
b) Legislação e estatutos vigentes;
c) Conjuntos particulares de princípios, objetivos e requisitos.

Toda informação acessada, armazenada, compartilhada e divulgada pelo Ribeiro de Andrade passa pela avaliação de riscos descrita nesta PSI, seguindo todos os critérios definidos pela ABNT NBR ISO/IEC 27002:2013. Os controles são separados por categoria, sendo que, cada seção possui seus objetivos, podendo ser um ou mais, suas diretrizes para implementação e informações adicionais, caso tenha.

2. CONSCIENTIZAÇÃO E TREINAMENTO

A PSI estará sempre disponível na intranet do Escritório, bem como divulgada no sítio na internet – ribeirodeandrade.adv.br. Ocorrerá conscientização e treinamento periódico, com o mínimo de uma vez ao ano, destinados aos “integrantes”, quais sejam, sócios, advogados associados, estagiários e funcionários e, caso necessário, à terceiros. Tais treinamentos serão divulgados previamente, sendo formalizados e avaliados.

3. RESPONSÁVEL PELA SEGURANÇA DA INFORMAÇÃO

Pedro Manetta Bicalho de Lana, administrador, RG MG 16.288.110, CPF 114.585.376-50 é nomeado o responsável pela segurança da informação (“DPO”), devendo: (i) definir e garantir a aderência da empresa às diretrizes de Segurança da Informação; (ii) mapear as ameaças significativas ao ambiente e risco de exposição da informação; (iii) garantir a conscientização de todos os funcionários e terceiros.

4. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações são classificadas levando em consideração quatro aspectos, quais sejam, a integridade, a disponibilidade, a confidencialidade e o valor. Para tanto, são divididas em níveis de segurança: (i) irrestritas, aquelas que são públicas, como as expostas no sítio da internet; (ii) internas, aquelas que o Escritório decide não divulgar para terceiros, pois podem ser estratégicas para a organização; (iii) confidenciais, divulgadas somente entre os sócios e a alta administração, pois podem causar danos financeiros ou à imagem; (iv) secretas, que são as informações vitais e restritas a um grupo seleto.

5. REUTILIZAÇÃO OU DESCARTE SEGURO DE EQUIPAMENTOS

As informações ficam armazenadas em dispositivos, tais como discos rígidos e mídias removíveis. A depender do nível de segurança da informação, esta encontra-se somente em discos rígidos, controlados por criptografia. Todo descarte de equipamento é acompanhado pelo responsável pela segurança da informação, bem como pelo responsável de tecnologia de informação, sendo formatado e, caso necessário, destruído, objetivando o descarte correto das informações ali encontradas.

6. CONTROLE DE ACESSO FÍSICO

Todos os funcionários e visitantes possuem crachá de identificação, sendo indispensável sua utilização para adentrar as dependências do Escritório. A área do datacenter é trancada por cadeado, apenas o responsável pela segurança da informação e o responsável pela tecnologia de informação possuem a chave de acesso. A entrada e saída de equipamentos possui procedimento uniformizado, sendo necessária a autorização do responsável pela segurança da informação.

O cabeamento de rede dos dispositivos que não possuem placa de rede Wi-Fi está devidamente trancado por rack, exceto se estiverem em manutenção. A

manutenção é realizada exclusivamente pelo responsável pela tecnologia de informação.

7. MESA LIMPA

As impressoras devem estar sempre em sala independente, sendo terminantemente proibido ficar em sala com colaboradores. Os documentos que contenham informações sensíveis devem ser removidos das impressoras, imediatamente. Também é proibido entrar na sala do Datacenter com pertences que possam ser utilizados para saída de informação. A entrada da sala do Datacenter é monitorada permanentemente por CFTV. As imagens ficam retidas pelo período de 90 dias.

8. PLANO DE CONTINUIDADE DO NEGÓCIO (“PCN”)

O Escritório mantém PCN conforme normas da Safety Culture, mantendo duas estruturas físicas distintas e relativamente distantes uma da outra, bem como hardware's de backup em localizações distintas. Os documentos são arquivados na Intranet e em software de nuvem terceirizado. O backup é realizado diariamente e mantido pelo prazo mínimo de três anos.

9. LEI GERAL DE PROTEÇÃO DE DADOS (“LGPD”)

A Lei 13.709/2018, popularmente conhecida como Lei Geral de Proteção de Dados entrou em vigor no território brasileiro, com o objetivo “de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”. O Escritório está ciente da aplicabilidade da referida Lei e para tanto, mantém DPO e as normas acima mencionadas, com o intuito de proteger os dados que são compartilhados com este.

Desse modo, toda atividade de tratamento de dados realizado pelo Escritório, envolvendo dados classificados como pessoais e sensíveis, pertencentes aos integrantes, colaboradores e clientes ao Escritório, ora pessoas naturais ou jurídicas, são realizados por plataformas seguras, baseados em um sistema de informação integrado, sendo, portanto, protegidos, independente do meio (físico ou digital), país de sede ou onde estejam localizados referidos dados.

Na hipótese de incidente de segurança da informação, o Escritório segue os seguintes passos: (i) avalia internamente o incidente – natureza, categoria e quantidade de titulares de dados afetados, categoria e quantidade dos dados afetados, consequências concretas e prováveis. Vide formulário de avaliação constante do site da ANPD; (ii) comunica o encarregado (Art. 5º, VIII da LGPD); (iii) comunica ao controlador, se for o operador, nos termos da LGPD; (iv) comunica a ANPD e ao titular de dados, em caso de risco ou dano relevante aos titulares (Art. 48 da LGPD); (v) elabora documentação com a avaliação interna do

incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas (Art. 6º, X da LGPD).

10. DISPOSITIVOS DE ARMAZENAMENTO

Diapositivos de armazenamento como discos rígidos, mídias removíveis, SSD's, etc, que contenham informação confidencial passam por processo de preenchimento de setores e equivalentes com zeros, eliminando os dados sem chance de recuperação, para serem descartados ou para assumirem outras funções.

11. GESTÃO DE MUDANÇAS

As demandas por mudanças de regras de firewall por parte dos usuários são formalizadas via e-mail para verificação da real necessidade pela equipe de TI. Sendo necessárias, são implementadas, após a realização de backup das regras vigentes. É uma situação rara, já que na maioria das vezes, as demandas são geradas pela própria equipe de TI e fornecedores de serviços como telefonia IP.

12. POLÍTICAS DE MALWARE

O Kaspersky Small Office é usado nas estações e servidores de arquivo. O CLAMD, antivírus Opensource, é utilizado no firewall pfSense. Os usuários não possuem acesso administrativo aos desktops e não conseguem fazer instalações. Os programas que rodam nos servidores e nos desktops são de licenças comerciais.

13. PATCHES DE SEGURANÇA

O Escritório trabalha apenas em dispositivos Windows, sendo as atualizações realizadas automaticamente pelas máquinas, através da ferramenta Windows Update.

14. BACKUP E RESTORE

O Escritório possui um servidor de backup em ambiente diverso do servidor principal, em outra instalação. Funciona com Ubuntu Linux e está isolado da rede SMB do Escritório como servidor, ou seja, atua como cliente no acesso ao servidor de arquivos, enquanto os discos de dados atuam como sistema de arquivos local.

Um script de backup copia os dados do servidor de arquivos para o servidor de backup em horários pré-definidos. Basicamente, o script sincroniza os dados dos discos do servidor de arquivos para o servidor de backup.

Também possui um sistema de versionamento de arquivos que gera snapshots duas vezes ao dia. Isso permite que um arquivo de dias anteriores seja recuperado.

15. DESATIVAÇÃO DE ESTAÇÃO DE TRABALHO

O Escritório segue os seguintes passos quando necessária a desativação de determinada estação de trabalho: (i) realização de backup das informações em área restrita no servidor de arquivos para posterior cópia no servidor de backup; (ii) retirada do servidor do domínio “randrade.intranet”; (iii) desinstalação do antivírus Kaspersky para liberação da licença; (iv) desinstalação do Microsoft Office para liberação da licença; (v) formatação do HD e utilização de ferramenta do fabricante para execução de procedimento "zero fill", preenchendo todos os setores do disco com zeros; (vi) guarda do PC em sala com acesso restrito.

16. CONFIDENCIALIDADE DAS SENHAS

Os colaboradores do Escritório têm ciência que as senhas fornecidas para acesso às máquinas e aos softwares são de uso pessoal e intransferível, devendo guarda-las somente para uso próprio, estando cientes, também, que o fornecimento para terceiros acarretará em sanções previstas nessa PSI.

17. SANÇÕES

Os colaboradores obrigam-se a expender todos os esforços e diligencias necessárias ao bom desempenho da função, no patrocínio das causas e tarefas que lhe forem confiadas, devendo manter absoluto sigilo sobre os fatos que tiver conhecimento, respondendo ilimitadamente pelos danos causados diretamente aos clientes, nas hipóteses de dolo ou culpa e por ação ou omissão, no exercício dos atos privativos da advocacia, sem prejuízo da responsabilidade disciplinar em que possa incorrer. O sigilo acima referido abrange todos e quaisquer dados e/ou informações considerados como privados e/ou restritos e/ou sigilosos à luz do ordenamento pátrio, inclusive, os albergados pelas Leis de Sigilo Bancário e de Proteção de Dados Pessoais.