POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Versão 1.1
Elaborado em: 10/06/2021
Última revisão em: 29/08/2022
Próxima revisão: 26/01/2023
Documento Público

Sumário

1 Objetivo 2
2 Princípios de Segurança da Informação 2
3 Informações Confidenciais 3
4 Controles e Gerenciamento de Segurança Cibernética 3
4.1 Gestão de Acesso às Informações 3
4.2 Proteção do Ambiente 4
4.2.1 Autenticação 4
4.2.2 Gestão de Incidentes de Segurança da Informação 4
4.2.3 Prevenção e detecção de Intrusão 4
4.2.4 Prevenção a Vazamento de Informação 4
4.2.5 Varreduras de Vulnerabilidades 5
4.2.6 Proteção contra Software Malicioso 5
4.2.7 Rastreabilidade 5
4.2.8 Acesso a Segmentação da Rede 5
4.2.9 Segurança - Copias de Backup 5
4.3 Continuidade de Negócios 5
4.4 Processamento, Armazenamento de Dados e Computação em Nuvem 6
4.5 Para a Contratação de Serviços de Terceiros em Nuvem 6
4.5.1 Controle de acesso 6
4.5.2 Gestão de Vulnerabilidade 6
4.5.3 Monitoramento dos Serviços 7
4.5.4 Gestão de Incidentes 7
4.5.5 Armazenamento de Dados 7
4.5.6 Continuidade de Negócios 7
4.5.7 Gestão e Retenção de Dados 7
4.5.8 Treinamento e Conscientização 8
4.5.9 Subcontratação de Serviços 8
4.5.10 Avaliações Periódicas 8
4.5.11 Sanções 8
5 Principais Recomendações de Segurança aos Usuários 9
5.1 Autenticações e Senhas 9
5.2 Antivírus 9
5.3 Engenharia Social 9
6 Vigência 10
7 Comunicação e Conscientização 10
8 Propriedade e Confidencialidade das Informações 10

1 Objetivo

A Política de Segurança da Informação e Cibernética ("Politica") da DOM PROCESSAMENTO DE DADOS LTDA ("DOM") tem o objetivo de garantir a proteção, manutenção da confidencialidade, integridade, disponibilidade de dados e sistemas da informação, de sua propriedade e/ou sob guarda, além de prevenir, detectar e reduzir vulnerabilidade a incidentes relacionados com o ambiente e incidentes cibernéticos, estabelecendo regras que representam em nível estratégico, os princípios fundamentais da DOM para o alcance dos objetivos de segurança da informação.

Esta Política visa estabelecer o compromisso da Diretoria da DOM em cuidar e tratar das informações, de forma a proporcionar segurança e privacidade dessas informações, estabelecendo regras gerais, em conformidade com as principais regulamentações vigentes.

Esta Política será aplicada na empresa DOM, obrigatório para todos os colaboradores[1] .

2 Princípios de Segurança da Informação

Consideramos que os ativos de informação são os bens mais importantes e devemos tratá-los com responsabilidade. A DOM está fundamentada nos princípios da segurança da informação, com o objetivo de preservação da propriedade da informação, assegurando sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos

Confidencialidade: garantia que a informação é acessível somente às pessoas autorizadas.

Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Acesso Controlado: garantia de que os acessos dos usuários à informação são restritos e controlados, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso.

[1] Todas as pessoas que desenvolvem algum tipo de atividade na DOM, com acesso aos softwares e equipamentos. Nesta categoria, enquadram-se funcionários CLT, estagiários e prestadores de serviços terceirizados.

3 Informações Confidenciais

O acesso às informações confidenciais, incluindo dados pessoais, coletados e guardados pela DOM é restrito aos profissionais autorizados ao uso dessas informações, sendo limitado o uso para outras tarefas.

A DOM poderá revelar as informações confidenciais nas seguintes hipóteses:

- Sempre que estiver obrigada a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial;
- Aos órgãos de proteção e defesa de crédito e prestadores de serviços autorizados pela DOM para defender seus diretos e créditos;
- Aos órgãos reguladores.

4 Controles e Gerenciamento de Segurança Cibernética

O gerenciamento de procedimentos e controles de Segurança Cibernética objetivam assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e mantidos ou modificados de acordo com os objetivos estabelecidos nessa Política.

Cada colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade.

Internet, e-mail e Computadores.

A DOM estabeleceu medidas buscando mitigar os riscos identificados, ou seja, impedir previamente a ocorrência de um ataque cibernético, incluindo programação e implementação de controles, na forma abaixo:

4.1 Gestão de Acesso às Informações

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

Os colaboradores e terceiros da DOM são treinados periodicamente sobre os conceitos de Segurança da Informação, através de um programa efetivo de conscientização e disseminação da cultura de segurança cibernética.

A DOM disponibiliza a seus Colaboradores uma completa estrutura material e tecnológica para exercício das atividades. É de responsabilidade do Colaborador manter e zelar pela integridade dessas ferramentas de trabalho.

Os equipamentos e instalações de processamento de informação crítica são mantidos em áreas seguras, com níveis de controle de acesso apropriados, inclusive contra ameaças físicas e ambientais.

4.2 Proteção do Ambiente

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes locais e internet, através de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e a administração segura de redes de comunicações.

4.2.1 Autenticação

O acesso às informações e aos ambientes tecnológicos da DOM, deve ser permitido apenas às pessoas autorizadas, levando em consideração o princípio do menor privilégio.

O controle de acesso aos sistemas deve ser formalizado e contemplar, no mínimo, os seguintes controles:

- Utilização de identificação (Controle de Acesso) individualizados, monitorado e passíveis de bloqueios e restrições. (automatizados ou manuais);
- A remoção de autorização dada a usuários afastados ou desligados; e
- Revisão periódica das autorizações concedidas.

4.2.2 Gestão de Incidentes de Segurança da Informação

O comportamento de possíveis ataques é identificado por meio de controles de detecção no ambiente, como filtro de conteúdo, ferramenta de detecção de comportamentos maliciosos, Antivírus, AntiSpam e outros.

4.2.3 Prevenção e detecção de Intrusão

Manter mecanismos de detecção que devem monitorar, analisar e bloquear ações realizadas com intuito de comprometer a estrutura básica da segurança de informação de um sistema informatizado, afetando sua integridade, confidencialidade e disponibilidade.

4.2.4 Prevenção a Vazamento de Informação

Manter um controle para prevenção de perda de dados, responsável por garantir que dados confidenciais não sejam perdidos, roubados ou vazados na web por usuários não autorizados.

4.2.5 Varreduras de Vulnerabilidades

As varreduras das redes internas e externas devem ser executadas periodicamente. As vulnerabilidades identificadas devem ser tratadas de acordo com seu nível de criticidade

4.2.6 Proteção contra Software Malicioso

Todos os ativos (computadores, servidores e outros) que estejam conectados à rede corporativa ou façam uso de informações da DOM, devem, sempre que compatível, ser protegidos com uma solução anti-malware, determinada pela equipe de TI.

4.2.7 Rastreabilidade

Manter trilhas de auditoria para todos os componentes de sistema para reconstruir os seguintes eventos:

- Autenticação de usuários (tentativas validas e invalidas);
- Acesso a Bancos de Dados;
- Ações executadas pelos usuários, incluindo criação ou remoção de objetos de sistema.

4.2.8 Acesso a Segmentação da Rede

- O acesso deve ser segmentado através de firewall, com segregação entre setores e servidores.
- Não é permitida a conexão direta de rede de terceiros, utilizando protocolos de controle remotos aos servidores conectados diretamente a rede corporativa;
- A criação, alteração ou exclusão de regras nos firewalls e ativos da rede, só poderão ser realizados pela Equipe de TI, após aprovação e análise.

4.2.9 Segurança - Copias de Backup

O processo de execução de backup é realizado diariamente, conforme descrito no documento ***Plano de Continuidade de Negócios***, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

4.3 Continuidade de Negócios

O processo de gestão de continuidade de negócios relativo à segurança da informação, é implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. O plano completo de contingência está descrito no documento ***Plano de Continuidade de Negócios***.

4.4 Processamento, Armazenamento de Dados e Computação em Nuvem

Os colaboradores externos da DOM, dentre os quais seus fornecedores, prestadores de serviços e parceiros, também podem representar uma fonte significativa de riscos de Cibersegurança. A computação em nuvem pode ser considerada como uma forma de serviços de terceiros e, assim como as demais contratações de Colaboradores externos, envolve determinados riscos e devem ser levados em conta pela DOM, demandando certos cuidados proporcionais a esta identificação de ameaças.

4.5 Para a Contratação de Serviços de Terceiros em Nuvem

O fornecedor que venha oferecer serviços em nuvem, processar ou armazenar dados da DOM em seu ambiente, deve seguir as seguintes diretrizes de segurança da informação:

4.5.1 Controle de acesso

- Possuir documentado um processo de Gerenciamento de Acesso;
- Dar acesso irrestrito aos dados e informações armazenadas ou a serem processadas, conforme os serviços específicos definidos, prezando pela confidencialidade, integridade, disponibilidade e pela capacidade de recuperação destes dados e informações; e
- Dar visibilidade aos procedimentos e controles utilizados para prestar os serviços, como descrito no item acima, em especial, para a identificação e a segregação de dados da DOM, por meio de controles físicos ou lógicos.

4.5.2 Gestão de Vulnerabilidade

- Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, envidando os seus melhores esforços e usando de procedimentos e controles, que abranjam, no mínimo a autenticação, a criptografia, a prevenção e detecção de intrusão, a prevenção de vazamentos de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidade, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação de rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

4.5.3 Monitoramento dos Serviços

- Assegurar que dispõe do mais alto nível de capacidade no provimento de informação e de recursos de gestão adequados ao monitoramento de serviços a serem prestados, bem como garantir o cumprimento da legislação e da regulamentação em vigor; e
- Informar e dar acesso a DOM, quando solicitado, sobre os recursos de gestão adequados ao monitoramento aos serviços contratados.

4.5.4 Gestão de Incidentes

- Manter processo estruturado a resposta a Incidentes;
- Quando solicitado, fornecer informações relacionadas a quantidade de incidentes ocorridos no período de 12 meses, classificando-os pela sua relevância;
- Manter a DOM permanentemente informada sobre eventuais limitações que possam afetar a prestação de serviços ou cumprimento da legislação e da regulamentação em vigor.

4.5.5 Armazenamento de Dados

- Informar e dar acesso ao grupo, quando solicitado, sobre as medidas de segurança para a transmissão e armazenamento dos dados e informações.

4.5.6 Continuidade de Negócios

- Definir um programa de continuidade de negócios, para assegurar que possíveis incidentes não afetem os serviços prestados à DOM, devendo para tanto manter ambiente de contingência para garantir a continuidade da prestação de serviços.

4.5.7 Gestão e Retenção de Dados

- Assegurar um processo de execução de backup periódico, armazenando informações da DOM, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

4.5.8 Treinamento e Conscientização

- Manter um programa anual de treinamento e conscientização em Segurança da Informação para todos os colaboradores, com reciclagem para os mais antigos e apresentação obrigatória aos recém-admitidos.
- Os terceiros que acessarem ou processarem dados pessoais e/ou informações sensíveis devem ter ciência desta Política e tudo que diz respeito ao treinamento de Segurança da Informação disponibilizado pela empresa.

4.5.9 Subcontratação de Serviços

- Notificar, de imediato, sobre a subcontratação de serviços relevantes;

4.5.10 Avaliações Periódicas

- A DOM poderá realizar, sempre que achar necessário, avaliações para atestar sobre a efetividade da implementação dos controles apresentados neste documento, devendo para isso comunicar o parceiro com 30 dias de antecedência.

4.5.11 Sanções

- A violação ou a não-aderência à ***Política de Segurança da Informação e Cibernética*** e suas definições será considerada falta grave, podendo ser aplicadas penalidades ou sanções cabíveis de acordo com as políticas da empresa.

5 Principais Recomendações de Segurança aos Usuários

5.1 Autenticações e Senhas

Serão fornecidas aos colaboradores senhas para acesso aos computadores, à rede corporativa, aos sistemas e ao correio eletrônico corporativo. Em nenhuma hipótese as senhas deverão ser transmitidas a pessoas que não sejam colaboradores, sendo os colaboradores responsáveis pela manutenção de cada senha e suas características.

Principais recomendações:

- Mantenha a confidencialidade, memorize e não registre a senha em lugar algum. Ou seja, não contar a ninguém e não anotar em papel;
- Alterar a senha sempre que existir qualquer suspeita de comprometimento dela;
- Elaborar senhas fortes, de modo que sejam complexas e de difícil adivinhação;
- Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ “logado” com sua identificação;
- Bloquear sempre o computador ao se ausentar;
- Sempre que possível, habilitar um segundo fator de autenticação (SMS, Token, etc.).

5.2 Antivírus

Todos os equipamentos de computadores e servidores devem manter uma solução de antivírus atualizada e instalada pela equipe de TI, como também possuir sistema operacional atualizado com as últimas atualizações realizadas.

5.3 Engenharia Social

Engenharia social, no contexto de segurança da informação, refere-se à teia pela qual uma pessoa procura persuadir outra, muitas vezes na ingenuidade ou confiança do usuário, objetivando, aplicar golpes ou obter informações sigilosas.

Seguem as mais conhecidas:

- **Pharming:** direciona o usuário para um site fraudulento, sem o seu conhecimento.
- **Phishing:** links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais.
- **Vishing:** simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais.
- **Smishing:** simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais.
- **Spam:** São e-mails não solicitados, os quais são enviados para muitas pessoas possuindo tipicamente conteúdo com fins publicitários. Além

disso, os Spams estão diretamente associados a ataques de segurança, sendo eles um dos principais responsáveis pela propagação de códigos maliciosos, venda ilegal de produtos e disseminação de golpes.

- **Acesso pessoal:** pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.
- **Fraudes Externas e invasões:** Realização de operações por fraudadores, utilizando-se de ataques em contas de clientes, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.
- **Ataques DDoS e Botnets:** Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos Botnets, o ataque vem de muitos computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

6 Vigência

Esta Política poderá ser revisada anualmente, ou, quando necessário, caso haja alguma mudança nas normas da DOM ou alterações de diretrizes de segurança da informação.

7 Comunicação e Conscientização

A presente Política deve ser divulgada a todos os colaboradores, prestadores de serviços e publicada no site da DOM, de forma que seu conteúdo possa ser consultado a qualquer momento.

8 Propriedade e Confidencialidade das Informações

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional realizada em nome da Coinvalores deve ser considerada confidenciais, e constituem ativo da Coinvalores, mesmo após término de contrato, sendo essencial à condução de nossos negócios, e não podem ser copiadas ou de qualquer forma retiradas do nosso sistema.