Política de Segurança da Informação

Sumário

1. Regra Geral

A Promofarma e suas unidades serão tratadas neste em outros documentos como Organização. Funcionários, estagiários, contratados e terceirizados serão tratados como colaboradores.

Todas as políticas relacionadas à de Segurança da Informação precisam estar disponíveis em local de acesso facilitado aos colaboradores, com versões controladas, protegidas contra alterações e devidamente classificadas quanto ao seu acesso e uso. Esta política é revisada e divulgada aos colaboradores anualmente.

2. Princípios de Segurança da Informação

O compromisso da Organização, com o tratamento adequados das informações, está fundamentado nos seguintes princípios:

- **Confidencialidade**: garantimos que o acesso à informação seja obtido somente por pessoas autorizadas e quando for necessário;
- **Disponibilidade**: garantimos que as pessoas autorizadas tenham acesso à informação sempre que necessário;
- **Integridade**: garantimos a exatidão e a completude da informação e dos métodos de seu processamento;
- **Confiabilidade**: garantimos a transparência no trato com os públicos envolvidos.

3. Diretrizes Gerais

Aplica-se esta Política a todas as informações presentes na Organização, que podem existir de diversas maneiras:

- Escrita em papel;
- Armazenada e/ou transmitida por meios eletrônicos;
- Exibida em filmes ou na mídia;
- Falada em conversas formais e informais.

Independente da forma ou o meio pelo qual a informação for apresentada/compartilhada, ela sempre deverá estar protegida adequadamente, de acordo com controles definidos neste documento.

Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas pelos usuários na utilização dos sistemas de informação na Organização.

As informações, inclusive as de propriedade intelectual, devem ser utilizadas apenas para os propósitos da Organização. Os usuários não podem, em qualquer hipótese, apropriar-se dessas informações, seja em CDs, pen drives, dispositivos móveis ou qualquer outra mídia de armazenamento de dados, ou realizar transmissões não autorizadas. Todos os documentos produzidos, por qualquer sistema de informação, na Organização são de propriedade exclusiva da Organização.

A identificação do usuário (por meio de seu usuário de rede, senha, crachá ou qualquer outro meio) é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas utilizando tal identificação. A liberação de seu uso será dada a partir do aceite e do preenchimento correto do Termo de Responsabilidade para Segurança da Informação (Anexo 1).

Todo processo de negócio ou de suporte, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de um colaborador ou equipe de colaboradores, para que a atividade não seja executada e controlada pelo mesmo colaborador ou equipe.

A Organização, por meio de suas áreas ou representantes de Tecnologia da Informação, se reserva o direito de monitorar e realizar auditorias, automaticamente, sobre o tráfego efetuado através das suas redes de comunicação, acesso à Internet, uso do correio eletrônico, pastas locais de rede, entre outros, em obediência às normas e procedimentos escritos neste e em outros documentos.

Todas as informações geradas internamente e as compartilhadas para o mundo exterior à Organização, deverão receber uma classificação de uso (“Uso Restrito”, “Confidencial”, “Uso Interno” ou “Uso Público”), para que haja proteção adequada quanto ao seu acesso e uso.

Periodicamente são realizados treinamentos sobre a política atual de Segurança da Informação, ou sempre que alterações significativas sejam inseridas. Nestes treinamentos também são passadas boas práticas e proteção e segurança de dados como políticas de Mesa limpa e Tela limpa.

4. Tratamento da Informação

A informação deve receber proteção adequada em observância aos princípios e diretrizes de Segurança da Informação da Organização em todo o seu ciclo de vida, que compreende:

- Geração;
- Manuseio;
- Armazenamento;
- Transferência;
- Transporte; e
- Descarte

Maiores detalhes sobre o ciclo de vida da informação, pode ser obtida na Política de Classificação da Informação.

5. Processo de Segurança da Informação

Para assegurar que as informações tratadas estejam adequadamente protegidas, a Organização adota os seguintes processos:

• Gestão de Ativos da Informação

Entende-se por ativos da informação tudo o que pode criar, processar, armazenar, transmitir e até excluir informação, podendo ser tecnológicos (software e hardware) e não tecnológicos (pessoas, processos e dependências físicas). Considera-se ativo ou recurso de processamento da informação, além de computadores, notebooks, servidores de dados, de aplicação, Web e de Correio eletrônico, sua infraestrutura de comunicações e processamento, assim como os chamados dispositivos móveis (smartphones, câmeras, gravadores e equivalentes) ou mídias removíveis (pen-drives, cartões de memória, HD externo, Cloud-drives ou equivalentes).

Os ativos são identificados de forma individual, inventariados e protegidos de acessos indevidos, fisicamente e logicamente, e tem documentação e planos de manutenção atualizados anualmente. Sua nomenclatura é composta por 3 partes:

- Tipo do equipamento;
- Identificação do local de instalação;
- Número sequencial de identificação.

Métodos de proteção e segurança são aplicados aos ativos da informação para proteger acessos indevidos ou não autorizados, vindos de meio externo ou internos, como dispositivos móveis ou mídias removíveis. Estes dispositivos estão sob atenção especial e restrições para evitar infiltração de fragilidades ou facilitar vazamento de informações.

Não é permitido aos colaboradores ou outras partes alterarem a configuração entregue para utilização, ficando esta atividade restrita aos colaboradores da área de Tecnologia da Informação.

Os equipamentos pertencentes à Organização de uso pessoal/coletivo, servidores de dados e aplicativos, de qualquer porte, estão dotados de mecanismos de proteção contra vírus e malwares, com atualizações automáticas e na frequência determinada pela área de TI.

A utilização de softwares, programas, aplicativos e ferramentas de produtividade ou de suporte são definidas pela área de Tecnologia da Informação, não sendo permitido, aos colaboradores, realizar instalação ou alterações significativas nos recursos de processamento da informação existentes.

Havendo a necessidade de uso/aquisição de software, sistema, programa, aplicativo ou ferramenta específica, o colaborador deverá obter aprovação da área de Tecnologia da Informação, que após análise técnica, de performance e de segurança necessárias, poderá autorizar sua aquisição ou utilização. Toda e qualquer instalação destas será realizada pela área de Tecnologia da informação ou pelo seu fornecedor, sob supervisão da área de TI.

Instalações de softwares de qualquer natureza devem ser solicitadas à área de TI, que irá analisar o impacto dessa instalação, executando-a ou não, de acordo com o resultado dessa avaliação.

Cada área da Organização possui pastas de arquivos exclusivas, com acesso restrito a seus colaboradores, devendo ser utilizada de forma ética e responsável. Em casos específicos determinados colaboradores poderão receber pastas exclusivas para seu uso pessoal, respeitadas cotas de uso.

O uso de impressoras é uma concessão feita aos usuários, assim como correio eletrônico, acesso à Internet, entre outros, e não um direito. Disto decorre que seu uso deve ser realizado prioritariamente para atividades ligadas ao trabalho, quando em horário comercial ou de trabalho remoto, contribuindo e controlando sua utilização para a segurança da Organização, no tocante a vazamento ou acesso indevido a informações desta. Material impresso defeituoso ou inservível pode ser utilizado como rascunho, contanto que não apresente dados de uso restrito, confidencial ou que represente risco à Organização. Material impresso inservível de uso restrito, confidencial ou com conteúdo sensível deve ser destruído através de fragmentação e/ou incineração.

O transporte de mídias físicas de armazenamento (fitas de backup, HD externo, cartões de memória, Pen drives etc.), que não seja por meios eletrônicos, deve considerar controles de entrada e saída destas mídias dos locais de armazenamento primário para os de recuperação/guarda. Os controles de entrada e saída devem considerar a solicitação e autorização de transporte/transferência da mídia, o registro do tipo de mídia física, o receptor/remetente autorizado, a data e o horário, e o número da mídia física. Deve-se aplicar proteção física extra a estas mídias, como envelopes selados/lacrados, para elevar o nível de proteção em seu transporte. Tais recursos devem ser aplicados para assegurar que os dados somente possam ser acessados no ponto de destino e não durante o transporte.

Procedimentos de criptografia a mídias físicas que contenham Dados Pessoais devem ser aplicados nos recursos de processamento da informação, em dispositivos móveis de armazenamento de dados e durante o transporte destes dados.

O descarte de recursos de processamento da informação considera:

a) Substituição de dispositivos de armazenamento de dados – a mídia substituída deve ser formatada utilizando recursos do sistema operacional e, se possível, métodos extras de destruição do seu conteúdo. Caso tenha que ser mantida por um tempo, antes do descarte de seu conteúdo, recomenda-se o uso de envelopes lacrados para sua guarda;
b) Destruição de dispositivos de armazenamento de dados – o processo de destruição da mídia deve considerar a adoção da legislação de proteção ao meio ambiente, uso de mecanismos físicos como furadeiras, martelo ou prensa mecânica/hidráulica, com objetivo de impedir totalmente o acesso indevido à mídia de armazenamento, ou seja, furar várias vezes os discos, esmagar as placas de dados e/ou os discos, entre outros;
c) Fragmentar ou incinerar documentos ou mídias não óptico/magnéticas.

• Procedimentos de backup

Estabelece diretrizes e padrões para os procedimentos de backup, testes e recuperação de dados como atividades periódicas ou realizados em caso de crise. Serão executados de forma automática e abrangem os dados gravados em sistemas, aplicativos, ferramentas, diretórios de rede privativos de cada equipe, nos servidores de dados e aplicativos.

Os dados armazenados em discos rígidos locais e pastas de rede de uso individual, não serão copiados e não será garantida sua recuperação em caso de erro físico nas mídias de gravação ou instabilidade no sistema operacional instalado no equipamento.

Dados armazenados em pastas individuais da rede, não terão garantida de sua recuperação, em caso de erro físico nas mídias de gravação ou instabilidade no sistema operacional ou de armazenamento corporativo.

Dados armazenados em pastas locais da rede terão suas cópias realizadas, segundo as diretrizes específicas da área de Tecnologia da informação.

A periodicidade, o tempo de retenção, o RPO (Recovery Point Objective) e o RTO (Recovery Time Objective) dos backups observam as regras especificadas nos contratos de prestação de serviços com fornecedores.

RPO (Recovery Point Objective): Tempo máximo suportado de perda de dados de um determinado serviço ou processo de negócio após a ocorrência de um desastre.
RTO (Recovery Time Objective): Tempo máximo para retorno operacional de um serviço ou processo de negócio após a ocorrência de um desastre.

• Transferência de informações/dados

Estabelece diretrizes e padrões para os procedimentos de transferência de dados interna e externamente, com proteção e segurança, através de análises e investigação de vulnerabilidades prévias, nos recursos de processamento da informação, permitindo correções/adequações a tempo, minimizando violação de dados e impedindo o vazamento dos dados tratados.

As diretrizes, padrões e recursos adotados constam de itens técnicos dos contratos com fornecedores.

• Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis:
(a) Restrito;
(b) Confidencial;
(c) Interno e
(d) Público.

Todas as informações necessárias para entender a Classificação da Informação está disponível na Política de Classificação da Informação, de Uso Interno, e disponível para consulta.

Segue abaixo descrição pormenorizada da Classificação da Informação:
a) Informação Restrita

É toda informação associada aos interesses estratégicos da Organização, de posse da diretoria, dos comitês e dos gestores das áreas. Seu acesso deve ser limitado a um número reduzido de pessoas autorizadas. Se revelada ou adulterada, pode trazer sérios prejuízos financeiros, favorecer a concorrência e gerar impactos negativos nos negócios ou na imagem da instituição ou dos demais agentes da organização. Essas informações requerem medidas de controle e proteção rigorosas contra acessos, cópias ou reproduções não autorizadas. Em geral, seu acesso é limitado à diretoria, gerentes das áreas, jurídico, auditoria e colaboradores previamente designados.

b) Informação Confidencial

É toda informação cujo conhecimento está limitado a colaboradores que, pela natureza da função que desempenham, dela necessitam para o exercício profissional. Sua divulgação ou adulteração pode trazer impactos negativos aos negócios e na gestão de processos, ou prejuízos à imagem da instituição ou aos demais agentes da organização.

c) Informação de Uso Interno

É toda informação cujo conhecimento e uso, estão restritos exclusivamente ao ambiente interno e aos propósitos da Organização, estando disponível aos colaboradores e podendo ser revelada ao público externo apenas mediante autorização do Dono/Gestor da Informação.

d) Informação de Uso Público

É toda informação que pode ser divulgada para o público externo à Organização, como imprensa, redes sociais, meios de comunicação etc., sem implicações de proteção e controle de acesso adicionais, tais informações somente serão publicadas com a permissão ou ser realizada pelas áreas de RH e Marketing.

IMPORTANTE: Na classificação de um conjunto de informações que apresentam diversos níveis de confidencialidade, deve-se adotar a classificação de maior nível presente no conjunto. Para isto, devem ser consideradas as necessidades relacionadas aos negócios, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

IMPORTANTE: A classificação será atribuída inicialmente pelo Dono/Gestor da Informação devendo ser obedecida por quem recebê-la.

A identificação da classificação da informação deve ser aplicada a todas as comunicações externas ou internas à Organização, seja como imagem ou texto, no rodapé dos e-mails, documentos ou apresentações, no caso de documentos em papel deverá estar destacada.

• Gestão de Acessos

As concessões, revisões e revogações de acesso utilizam ferramentas e processos da Organização e estão baseadas em um fluxo de solicitação, aprovação, análise e execução.

Os acessos a recursos de processamento da informação ou a ambientes físicos, devem ser rastreáveis, a fim de garantir que todas a ações passíveis de auditoria possam identificar individualmente o colaborador, suas ações e permissões, para sua devida responsabilização.

Devem estar habilitados logs de acesso a recursos de processamento da informação, como:

- Estações de trabalho (desktop e notebook)
  - Log-in e log-off;
- Servidores de dados, aplicativos, WEB e de comunicações
  - ID usuário,
  - data e hora de acesso,
  - identificação do recurso de processamento da informação,
  - operação realizada,
  - resultado da operação (sucesso ou não);
- Sistemas, ferramentas e aplicativos
  - ID usuário,
  - data e hora de acesso,
  - identificação do sistema, ferramenta, aplicativo,
  - módulo, funcionalidade, opção utilizada,
  - operação realizada (inclusão, alteração, exclusão, consulta, emissão de relatório, cópia etc.),
  - Se alteração - informação anterior e informação resultante,
  - Se exclusão – informação eliminada,
  - Se consulta, impressão ou cópia – informações apresentadas para a operação,
  - resultado da operação (sucesso ou não);
- Configuração de sistema operacional, antivírus, malware, Endpoint, ERP, outros
  - ID usuário,
  - data e hora de acesso,
  - identificação do recurso acessado,

- parâmetro acessado/alterado,
- operação realizada (inclusão, alteração, exclusão, consulta, emissão de relatório, cópia etc.),
- informação resultante da operação

As trilhas de auditoria de sistemas devem ser definidas pelos Donos da Informação (conforme Política de Classificação da informação), seu tempo de retenção e método de eliminação. A equipe de TI ou de Segurança da Informação deve definir o espaço máximo de armazenamento para estas trilhas de auditoria, local de armazenamento, acesso apenas de leitura sob demanda e aprovação, mecanismos de backup distintos, gestão das trilhas de auditoria.

Periodicamente devem ser realizadas revisões de acessos sobre os recursos de processamento da informação e ambientes físicos, que consideram os recursos de processamento da informação, módulos, funcionalidades, usuários, permissões concedidas e capturar, dos gestores destes recursos, novas concessões, revogações ou manutenção das permissões existentes.

• Gestão de Riscos

Os riscos devem ser identificados e classificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação, sobre os processos de negócios ou de suporte, sobre os tratamentos de dados realizados e sobre o relacionamento com fornecedores e/ou prestadores de serviço da Organização, para que sejam recomendadas as ações de implementação, correção e proteções adequadas/necessárias.

A identificação dos cenários de riscos de Segurança da Informação, processos de negócio e de suporte, tratamento de dados e sobre o relacionamento com fornecedores e/ou prestadores de serviço, além das ações a serem tomadas, serão discutidas nos comitês específicos da Organização, conforme diretrizes de Governança Corporativa adotadas.

Os testes de identificação de vulnerabilidades e fragilidades na infraestrutura interna e externa da Organização, são realizados periodicamente e seus resultados são avaliados pela alta direção, tendo seus planos de ação considerados e adotados conforme deliberação destes comitês.

Deve-se manter, junto à equipe de Compliance da Organização, uma Matriz de Riscos, identificando os riscos, suas causas, controles de identificação de materialização e planos de ação, juntamente com a gestão compartilhada sobre a execução e eficácia destes planos de ação, juntamente com a identificação dos responsáveis, sua data de conclusão, grau de efetividade e risco residual.

• Tratamento de Incidentes de Segurança da Informação e Segurança Cibernética

Os incidentes de segurança da informação e cibernéticos da Organização devem ser reportados à área de Segurança da Informação/Tecnologia da Informação, seja pessoalmente, por e-mail ou qualquer outra forma existente, conforme processo estabelecido, imediatamente e sem restrições ou receio de penalidades. O tratamento destes incidentes está mapeado em um processo exclusivo de Gestão de Incidentes de Segurança da Informação, sob responsabilidade de Segurança da Informação/Tecnologia da Informação. Sua gestão será realizada em processo específico de Gestão de Incidentes de Segurança da Informação.

Eventos identificados e classificados como de vazamento ou violação de dados, serão tratados como um subprocesso da Gestão de Incidentes de Segurança da Informação, devendo ser reportados ao Encarregado de Proteção de Dados da Organização (DPO), imediatamente, pessoalmente, por e-mail ou qualquer outro meio disponível, para que este realize a gestão deste processo, tome as providências necessárias, comunique às partes interessadas e realize as análises, tome as ações adequadas, documente o evento, finalize o evento e adote um processo de melhoria contínua do processo.

• Governança com as Áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócios e tecnologia devem estar alinhadas com as diretrizes e arquiteturas de Segurança da Informação, garantindo a confidencialidade, integridade, disponibilidade e confiabilidade das

informações. São tratadas em processo específico de Gestão de Demandas e projetos, devendo estar alinhadas às diretrizes da Organização, conforme determinado pelas ações adotadas segundo a Governança Corporativa.

• Segurança Física do Ambiente

O processo de segurança física estabelece controles relacionados à proteção física do perímetro da Organização, à concessão de acesso físico aos ambientes, somente a pessoas autorizadas, de acordo com a criticidade das informações previamente mapeadas e declaradas. Estabelece critérios e controles de monitoração do ambiente físico, métodos de comunicação e restrição de colaboradores e terceiros aos ambientes seguros da Organização.

• Segurança Cibernética

A segurança cibernética da Organização é norteada pelos seguintes fatores:
(a) Regulamentações vigentes;
(b) Melhores práticas; e
(c) Cenário mundial.

Conforme sua criticidade, o programa divide-se em:

a) Ações críticas: Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;
b) Ações de Sustentação: Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da Organização e permitindo que ações de longo prazo ou estruturantes possam ser realizadas;
c) Ações Estruturantes: Iniciativas de médio/longo prazo que tratam a causa raiz dos riscos e que preparam a Organização para o futuro.

Ações de suporte da equipe de colaboradores da área de Tecnologia da Informação através de ferramentas de acesso remoto às estações somente poderão ser realizadas através da solicitação do usuário, com aprovação de seu gestor imediato e análise pela equipe de Tecnologia da Informação.

Medidas protetivas ao acesso remoto às redes da Organização, seja por conexão direta, através de VPN ou ferramenta de acesso remoto, devem ser mantidas atualizadas e validadas periodicamente, alinhadas às diretrizes do Plano de Continuidade de Negócios.

6. Normas de Utilização da Internet

O acesso à Internet na Organização é uma concessão feita aos usuários, e não um direito. Disto decorre que se deve utilizá-la prioritariamente para atividades ligadas ao trabalho, quando em horário comercial ou de trabalho remoto.

Os usuários devem utilizar a Internet de forma adequada e diligente, em conformidade com a lei, a moral e a ordem pública, abstendo-se de objetivos ou meio para a prática de atos ilícitos, lesivos aos direitos e interesses da Organização ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos e documentos de qualquer tipo.

É proibida a divulgação e/ou compartilhamento indevido de informações sigilosas em listas de discussão, bate-papo ou softwares de mensagens eletrônicas, externos à Organização.

A concessão de uso será realizada a partir de uma solicitação registrada na ferramenta de chamados, pelo colaborador, com aprovação pelo gestor da área e validação/aprovação pela equipe de TI.

Usuários com acesso à Internet não podem e não devem efetuar upload, para a Internet ou qualquer outro local/meio, de qualquer software/arquivo/documento cuja licença pertença à Organização, o mesmo ocorrendo para dados/processos/informações de propriedade da Organização. Exceção feita a casos especiais, mediante solicitação do interessado ao responsável pelo software/dado/documento, conforme Política de Classificação da informação, e sua posterior autorização e análise autorização pela equipe de Tecnologia da Informação.

Downloads serão autorizados, mediante solicitação, justificativa e aprovação prévias, conforme processo de solicitações/chamados estabelecido, desde que a fonte seja confiável. Para instalação de softwares oriundos da Internet, será necessária autorização da área de Tecnologia da Informação.

Cada usuário é responsável por zelar pelo cumprimento ao estabelecido pela presente norma e por todas as atividades realizadas por intermédio de seu usuário de rede. As contas de serviço (grupo) têm acesso restrito a determinadas pastas e recursos de rede da Organização.

Não é permitida a utilização de Webmail externo (não homologado pela equipe de TI), salvo autorização pela área de TI, não é permitido uso software peer-to-peer (comunicação ponto-a-ponto, torrente ou equivalente), não é permitido acesso a sites de relacionamento (Facebook, Twiter, Instagram e afins), não é permitido acesso a conteúdo de pornografia/pedofilia e outros contrários à lei ou normativos internos, como o Código de Conduta e Ética.

7. Normas de Utilização da Telefonia

De acordo com a regulamentação interna, as ligações telefônicas realizadas não são monitoradas e gravadas. O que não exime cada colaborador ou prestador de serviços, usuário deste serviço de seguir as regras de comportamento público do Manual de Conduta e Ética da Organização.

8. Normas de Utilização do Correio Eletrônico

As contas de correio-eletrônico têm titularidade única e exclusiva, sendo considerada como uma ferramenta de trabalho, e seu bom ou mal uso determina a responsabilidade direta do usuário. As contas de serviço (grupo), por sua vez, possuem um ou mais responsáveis pelo seu uso.

A utilização do correio deve ser feita de forma adequada e diligente, exclusivamente para atender aos fins da Organização. A concessão de uso será realizada a partir de uma solicitação registrada na ferramenta de chamados, realizada pelo gestor da área solicitante, com análise e aprovação pela equipe de TI.

O tamanho das caixas postais é de 30GB para usuários todos os usuários. Já em relação ao tamanho de cada mensagem enviada/recebida, o limite é de 10MB. Necessidades acima destes limites devem ser solicitados à área de Tecnologia da Informação.

É vedada a qualquer usuário a utilização do correio eletrônico para quaisquer das seguintes atividades:

- Envio de mensagens não autorizadas, divulgando informações sigilosas;
- Acesso não autorizado à caixa postal de outro usuário ou de serviços, caso esta não esteja sob sua responsabilidade;
- Envio, manuseio e armazenamento de material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos (seja pela lei, seja pela presente norma ou Código de Conduta e Ética), lesivos aos direitos e interesses da Organização, que possam danificar, inutilizar, sobrecarregar ou deteriorar hardware e/ou software, documentos e arquivos de qualquer tipo, ou que contrariem a moral, os bons costumes e a ordem pública;
- Envio intencional de mensagens do tipo “corrente”, “spam” ou que contenham vírus eletrônico ou qualquer forma de programação (arquivos executáveis ou do tipo script) que sejam prejudiciais ou danosas aos destinatários das mensagens;
- Utilização de listas e/ou caderno de endereços para distribuição de mensagens que não tenham relação com o interesse funcional da Organização ou a devida permissão do responsável pelas listas e/ou caderno de endereços em questão;
- Uso de contas particulares, através da configuração dos serviços Post Office Protocol – POP, Internet Message Access Protocol – IMAP e Simple Mail Transfer Protocol – SMTP de provedores não pertinentes aos domínios pertencentes à Organização.
- Envio de mensagens que contenham arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança da rede;

- Todo e qualquer uso do correio eletrônico não previsto nesta política que afete a Organização de forma negativa.

9. Normas de Utilização de Contas e Senhas para Usuários

Com o intuito de controlar a distribuição de direitos de acesso a sistemas de informação e serviços, a Organização estabelece estas normas para evitar o uso inapropriado de usuários e senhas e, consequentemente, diminuir o risco de falhas e violações de sistemas.

9.1. Usuário e senha forte

Todos os usuários e senhas de rede são **pessoais e intransferíveis**, **devendo ser mantidas em sigilo**. Cada usuário é responsável por manter em segredo seu usuário e sua senha, e será responsabilizado pelo mau uso desses.

As senhas de rede para usuários finais têm, no mínimo, 8 caracteres, sendo obrigatório o uso de letras maiúsculas e minúsculas, números e caracteres especiais (@ % ^; .), na ocorrência de 5 tentativas de ingresso erradas, a senha de acesso à rede da Organização é bloqueada. Para desbloqueio, somente com solicitação formal à área de TI. O tempo de expiração da senha será de 60 dias no máximo, podendo ser trocada a qualquer momento pelo colaborador. O desbloqueio de usuários e senhas somente ocorrerá através de solicitação formal pelo gestor imediato do colaborador.

Quaisquer desligamentos ou novas contratações deverão ser informados com antecedência às áreas de Segurança da Informação/Tecnologia da Informação e representantes de Compliance/Controles Internos, para que os acessos à Organização sejam bloqueados ou concedidos adequadamente.

9.2. Criação de usuários

A criação ou alteração de usuários e atribuição de senhas será realizada a partir de uma solicitação registrada na ferramenta de chamados, pelo gestor da área solicitante ou representante de RH, quando da contratação de um colaborador. A primeira senha será criada já como expirada, exigindo que na primeira conexão do usuário essa seja trocada.

A identificação de usuário segue as seguintes regras:

- Primeiro nome, seguido de um ponto, seguido pela última parte do nome do colaborador
- Casos de duplicidade de identificação de usuário será utilizada outra parte do nome do colaborador

9.3. Condições gerais de usuários e senhas

Eventos de incidente de segurança da informação ou de vazamento/violação de dados, poderão iniciar um processo de expiração de senhas, conforme procedimento específico de Gestão de Incidentes de Segurança ou de Vazamento ou Violação de Dados.

Todos os sistemas e aplicações instalados na Organização devem ter algum mecanismo que oculte a visualização das senhas para utilização desses sistemas/aplicações.

Os usuários de rede terão privilégios administrativos que se enquadrem às suas atividades, o mesmo ocorrendo nas permissões aos diretórios de rede e seus conteúdos.

10. Normas de Controle de Acesso

O acesso físico às dependências da Organização e a segregação física das atividades está contemplado na Política de Segregação de Atividades.

11. Aprovação desta Política

A presente política foi revisada e aprovada pelo Comitê de Risco e Compliance.

Versão	Responsável	Aprovador	Data publicação
1.0			

ANEXOS

TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TERMO DE ADESÃO

Atesto ter recebido, lido e compreendido as diretrizes, normas, instruções e procedimentos contidos na Política de Segurança da Informação da Organização, comprometendo-me a observá-la em sua íntegra e comunicar, imediatamente qualquer inconformidade com a Política que venha a ser de meu conhecimento, seja diretamente, seja por terceiros.

Declaro ter pleno conhecimento que o descumprimento deste Termo de Adesão pode implicar no meu afastamento imediato da empresa, sem prejuízo da apuração dos danos que tal descumprimento possa ter causado.

Declaro ainda que, quando cabível, o descumprimento deste termo pode sujeitar-me às responsabilidades legais associadas a meus atos.

_____ ,___ de _____ de _____

_____

Assinatura e Nome Completo

Glossário

Usuário - Funcionários das Empresas Olavo Barbosa, que estão autorizados a utilizar a rede e os equipamentos de informática. Pode também, ser referenciado como uma identificação de usuário.

TI - Tecnologia da Informação (informática).

Recurso de processamento da informação - São os equipamentos utilizados pelos funcionários tais como: computadores, impressoras, e-mails, Internet e afins.

Identificação de Usuário – Identidade atribuída a um colaborador para realizar acesso aos recursos de processamento da informação da organização.

Site ou Website – Endereço na internet (WWW) composta por páginas que contém informações, imagens, vídeos, sons etc., para serem acessados por qualquer pessoa que se conecte à rede mundial. Estão hospedadas em servidores Web, que armazenam conteúdo, dados e outros tipos de informação, administradas por provedores de acesso.

Software – Programas de Computador

Download – Atividade de copiar conteúdo da internet para estação local de trabalho, dispositivos móveis (smartphones, câmeras, gravadores e equivalentes) ou mídias removíveis (pen-drives, cartões de memória, HD externo ou equivalentes), ou recurso de processamento da informação, através da Internet.

Upload – Envio de um arquivo de um recurso de processamento da informação para outro, através da Internet. **Peer-to-Peer** (P2P) – É um tipo de programa que permite a distribuição de arquivos a outros usuários através da Internet (exemplo Torrent).

Internet – Associação mundial de redes de computadores interligados, que utilizam protocolos de comunicação de dados. A Internet provê um meio abrangente de comunicação através de: transferência de arquivos, conexões à distância, serviços de correio eletrônico etc.

Intranet – Rede interna, restrita, de uso pessoal ou corporativo, que utiliza a mesma tecnologia da Internet, para que os usuários possam acessar as informações dos seus respectivos departamentos.

Caixa Postal – Recurso de armazenamento de dados de mensagens de correio eletrônico, onde são armazenadas as mensagens de e-mail e seus anexos.

Correio eletrônico – Meio de envio e recebimento de informações entre 2 ou mais partes, baseado em protocolos de comunicação da Internet, que se utiliza de uma rede comunicação de computadores.

FTP (File Transfer Protocol) – Protocolo padrão da Internet, usado para transferência de arquivos entre recursos de processamento de informação.

IMAP (Internet Message Access Protocol) – Protocolo de acesso a mensagens eletrônicas.

POP (Post Office Protocol) – Protocolo usado por clientes de correio eletrônico para manipulação de arquivos de mensagens em servidores de correio eletrônico

SMTP (Simple Mail Transfer Protocol) – Protocolo de comunicação usados para troca de mensagens na Internet.