Política Corporativa de Segurança da Informação

HISTÓRICO DE REVISÕES

Número da edição	**Elaborador** (Nome/data)	**Revisor** (Nome/data)	**Descrição da alteração**
01	Tania Maria Costacurta 12/07/2012	Pedro Balista 13/07/2012	Atualização do padrão de documentação de Política.
02	Fábio Tavares Szescsik 14/07/2015	André Guarenghi 15/07/2015	Revisão, atualização e simplificação da Política.
03	Edemar H. K. Luccezen 22/12/17	Nandor Feher 22/12/17	Revisão conteúdo monitorado.
04	Edemar H. K. Luccezen 18/06/18	André Guarenghi 18/06/18	Revisão conteúdo monitorado.
05	Edemar H. K. Luccezen 26/09/18	Nandor Feher 26/09/18	Revisão conteúdo.

OBJETIVO

A informação é, atualmente, um dos ativos mais valiosos de qualquer organização. Dessa forma, a Positivo Tecnologia estabelece a presente ***Política Corporativa de Segurança da Informação***, para a aplicação dos princípios e diretrizes de proteção das informações da empresa, dos clientes e do público em geral.

PÚBLICO-ALVO

Esta política destina-se a todos os colaboradores da Positivo Tecnologia, sejam eles: funcionários, estagiários, prestadores de serviços (terceiros), parceiros de negócio, visitantes da empresa ou qualquer pessoa que tenha acesso a qualquer ativo de informação.

RESPONSABILIDADES

Colaborador

É missão e responsabilidade de cada colaborador, observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente Política Corporativa de Segurança da Informação.

Área de Segurança da Informação

É missão da área de Segurança da Informação administrar as disciplinas de conhecimento que dão suporte a essa ciência, sendo responsável por editar as políticas e padrões que apoiam a todos na proteção dos ativos de informação, e estar preparada para auxiliar na resolução de problemas relacionados ao tema.

1 DIRETRIZES

1.1 Princípios de Segurança da Informação

Nosso compromisso com o tratamento adequado das informações, é fundamentado nos seguintes princípios:

Confidencialidade – somente pessoas autorizadas devem possuir acesso à informação, e quando de fato for necessário;

Integridade - a informação deve estar integra (possuir exatidão) e precisa, quando for necessária à sua utilização.

Disponibilidade – a informação deve estar disponível, sempre que o seu acesso for necessário por pessoas devidamente autorizadas.

1.2 Diretrizes gerais de Segurança da Informação

A Segurança da Informação da Positivo Tecnologia estabelece os principais controles:

- As informações da Positivo Tecnologia, dos clientes e do público em geral devem ser tratadas de forma ética, sigilosa, sempre estando de acordo com as leis vigentes e com as normas internas, evitando-se mau uso e exposição indevida.
- A informação deve ser utilizada de forma controlada e apenas para a finalidade para a qual foi coletada.
- O acesso às informações e recursos só deve ser feito se devidamente autorizado.
- A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas por meio de seu usuário/senha.
- A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades. Toda solicitação de acesso, deve possuir aprovação do gestor imediato do solicitante, ou seguindo plano de concessão do acesso específico.
- Os riscos às informações da instituição devem ser reportados à área de Segurança da Informação, por meio do e-mail: gsi@positivo.com.br.
- As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos colaboradores, que devem entender e assegurar estas diretrizes.

1.3 Tratamento de informações confidenciais

As informações confidenciais necessitam de sigilo absoluto e devem ser protegidas por cada colaborador. Falhas no sigilo da informação, integridade ou disponibilidade deste tipo de informação trazem grandes prejuízos à organização, expressos em perdas financeiras diretas, perdas de competitividade e produtividade ou degradação da imagem da Positivo Tecnologia.

São exemplos de informações confidenciais:

- Dados cadastrais (CPF, RG etc.), situação financeira, salários e movimentação bancária dos colaboradores.
- Informações sobre produtos e serviços que revelem vantagens competitivas da Positivo Tecnologia frente ao mercado.
- Todo o material estratégico da Positivo Tecnologia (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de

conhecimento de negócio da pessoa).

- Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades.

1.4 Uso de recursos computacionais

O uso de dispositivos pessoais, como desktops, laptops, tablets e smartphones para acesso as informações e conexão à rede corporativa da empresa, somente serão permitidos se autorizado previamente pela área de Segurança da Informação, mediante procedimento específico.

Fica proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação dos computadores e recursos tecnológicos, que não seja realizado por um técnico do setor de TI. As áreas de negócio que necessitarem fazer testes deverão solicitá-los previamente ao setor de Segurança da Informação, ficando o solicitante responsável jurídica e tecnicamente pelas ações realizadas.

É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico do setor de TI.

A utilização de softwares comerciais necessita de licença de uso válida, ou licença gratuita para o uso corporativo, devidamente homologados pela área de Segurança da Informação.

Ao furto ou roubo da propriedade intelectual alheia, damos o nome de “Pirataria”. A pirataria de software é a cópia, reprodução, uso ou fabricação não autorizada de softwares protegidos por leis e tratados internacionais e nacionais de direito autoral.

O colaborador responderá por qualquer procedimento administrativo, judicial, cível e/ou penal em decorrência do não cumprimento desta política.

1.5 Uso de e-mails

O uso do correio eletrônico é limitado ao suporte das atividades profissionais e uso pessoal dentro das expectativas apresentadas pela Positivo Tecnologia neste documento, seguindo as normas estabelecidas nos demais documentos complementares da Política Corporativa de Segurança da Informação.

É expressamente proibido o uso do sistema de correio eletrônico para o envio de correntes, mala-direta, mensagens com anúncio de eventos particulares, propagandas não solicitadas, vídeos, fotografias, música, ou qualquer tipo de mensagem que não tenha relação com as atividades da companhia.

O acesso ao e-mail por meio de dispositivos móveis, tais como tablets, celulares e smartphones, só será permitido se homologados pela área de Segurança da Informação, Telecom ou TI.

Todas as mensagens recebidas e enviadas através do sistema poderão ser monitoradas quanto a sua origem, destino, assunto e conteúdo através de ferramenta apropriada, e o responsável poderá receber auditoria a qualquer momento, sem qualquer aviso ou aprovação prévia do colaborador.

1.6 Uso da Internet

O uso da Internet é limitado ao suporte das atividades profissionais e ao uso dentro das expectativas apresentadas pela companhia neste documento e nas normas estabelecidas nos demais documentos complementares da Política Corporativa de Segurança da Informação.

É expressamente proibida à utilização da estrutura para atividades de compartilhamento ou distribuição de arquivos, seja apoiada por sistemas e/ou aplicações do tipo P2P, BitTorent, ou por qualquer outro que tenha esta funcionalidade.

É vetado todo tipo de download de arquivos (incluindo áudio e vídeo) e softwares sem a autorização da área de Segurança da Informação.

A utilização de sites de ***Streaming*** (YouTube, rádios online, NetFlix, etc) devem ser limitados a pesquisas ou atividades relacionadas ao trabalho do colaborador. A execução de *playlists* ou vídeos para fins particulares é vetada, devido ao risco de oneração e comprometimento dos recursos que utilizem a Internet, principalmente processos produtivos ou fiscais.

Todos os acessos realizados à Internet, pelos colaboradores da Positivo Tecnologia são armazenados e monitorados* pela área de Segurança da Informação, sem qualquer aviso ou aprovação prévia do colaborador.

Auditorias periódicas são realizadas visando manter a saúdo do ambiente, ficando a critério da equipe de TI a remoção dos acessos nocivos mesmo que devidamente autorizados.

*Seguindo a legislação vigente, nenhum site, aplicativo ou qualquer conexão relacionada a acessos bancários são monitorados.

1.7 Desvios à Politica vigente

As violações de segurança devem ser informadas à área de Segurança da Informação, que irá analisar o incidente ocorrido e determinar quais as medidas necessárias para que a falha seja corrigida e o processo reestabelecido. Toda violação estará sujeita a sanções, que podem variar desde uma advertência até o desligamento do colaborador da Positivo Tecnologia, inclusive por justa causa, de acordo com a quantidade de recorrências e/ou criticidade do desvio realizado.

São exemplos de desvios que podem ocasionar sanções:

- Uso ilegal de software.

- Introdução intencional de vírus de computador, na rede da empresa.
- Tentativas de acesso não autorizado a informações e sistemas.
- Compartilhamento de informações sensíveis do negócio.
- Uso indevido do e-mail, internet e demais recursos.
- Inserção de equipamentos não autorizados na rede da empresa.
- Desvio a qualquer um dos pontos apresentados por esta política.

1.8 Gestão da Segurança da Informação

Para uma adequada Gestão da Segurança da Informação da Positivo Tecnologia, estabelecemos os seguintes controles:

1.8.1 Gestão de Ativos da Informação

Os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos. Devem também possuir documentação adequada e planos de manutenção periódicas.

1.8.2 Gestão de Acessos

As concessões, revisões e exclusões de acesso devem usar as ferramentas e seguir os processos estabelecidos pela Positivo Tecnologia. Os acessos devem ser rastreáveis, para garantir que possamos identificar individualmente o colaborador, sendo esse responsabilizado por suas ações.

1.8.3 Gestão de Riscos

Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da Positivo Tecnologia, para que sejam recomendadas as proteções adequadas.

1.8.4 Tratamento de Incidentes de Segurança da Informação

Os incidentes relacionados as informações (utilização indevida, acessos não autorizados, etc.) devem ser reportados à área de Segurança da Informação, para o tratamento adequado.

1.8.5 Conscientização em Segurança da Informação

A Positivo Tecnologia promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura da Segurança da Informação.

1.9 Propriedade Intelectual

Todas as tecnologias, marcas, recursos, processos e metodologias, além de quaisquer informações que pertençam à Positivo Tecnologia não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio colaborador em seu ambiente de trabalho.

1.10 Declaração de Responsabilidade

Os colaboradores e prestadores de serviços diretamente contratados pela Positivo Tecnologia, devem aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de Segurança da Informação.

Os contratos firmados com a Positivo Tecnologia, devem possuir uma cláusula que assegure a confidencialidade das informações.

2 DOCUMENTOS RELACIONADOS

Esta Política Corporativa de Segurança da Informação é complementada por normas e procedimentos específicos de Segurança da Informação, em conformidade com os aspectos legais e regulamentares, das quais a empresa está sujeita.

3 ÓRGÃO RESPONSÁVEL

A área de Segurança da Informação é responsável por manter e atualizar esta política, bem como por manter a confidencialidade, integridade e disponibilidade das informações, por meio de ações de conscientização e treinamento, processos e também por meio de monitoramento das ações realizadas por cada colaborador.