Braspor Gráfica e Editora Ltda.

Política de Segurança da Informação

Versão 3.0 - 01 de setembro de 2017

INFORMAÇÕES CONFIDENCIAIS

Este documento é propriedade da Braspor Gráfica e Editora Ltda. e contém informações proprietárias, sendo restritas à divulgação não autorizada. A disseminação, distribuição, reprodução ou utilização total ou parcial deste documento por qualquer terceiro além da pessoa a quem ele se destina, sem a prévia autorização por escrito da Braspor Gráfica e Editora Ltda., está estritamente proibida.

Conteúdo

1 Objetivo

Este documento tem como objetivo explicar e estabelecer os requisitos de segurança da informação da Braspor Gráfica e Editora Ltda. para todos os colaboradores, prestadores de serviços e parceiros. A administração da organização adotou esta política de segurança para proteger a informação com o objetivo de atingir suas metas comerciais ou de conformidade com normas e leis aplicáveis.

2 Classificação do documento e alvo

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que utilizam, mantêm ou lidam com ativos de informação da organização.

3 Comitê de Segurança da Informação

O Comitê de Segurança da Informação tem por objetivo auxiliar na criação e revisão de políticas, normas e procedimentos gerais relacionados à segurança da informação. O comitê é formado por um grupo de gestores dos departamentos de Qualidade, Treinamentos, Tecnologia da Informação, Inkjet (dados variáveis) e Diretoria.

É responsabilidade do Comitê garantir a segurança da informação, a preservação dos ativos, a garantia de execução dos processos minimizando e mitigando riscos à organização. Para cumprimento deste propósito devem acontecer reuniões semestrais, exceto se convocadas por algum dos membros por demanda emergencial. As atas das reuniões serão assinadas por todos os membros presentes e arquivadas no departamento de Tecnologia da Informação.

O Comitê possui autonomia para debater e/ou recomendar quaisquer aspectos relacionados à segurança da informação, oferecendo subsídio à Diretoria no processo de tomada de decisão.

Caso haja necessidade, podem ser formadas comissões específicas para debater alterações dentro dos procedimentos contidos nesta política.

4 Responsabilidades dentro da Política de Segurança da Informação

4.1. Organizando a Segurança da Informação

Constitui-se nesta política a responsabilidade ao departamento de Tecnologia da Informação, conjuntamente com o Comitê de Segurança da Informação, de assegurar a seleção de controles de segurança adequados para proteger os ativos de informação e proporcionar confiança ao negócio onde a organização atua.

4.2. Papeis e Responsabilidades da Segurança da Informação

4.2.1 Gerente de Infraestrutura e Segurança

O Gerente de Infraestrutura e Segurança é responsável por coordenar e supervisionar o cumprimento das políticas e procedimentos em toda a organização no tocante à confidencialidade, integridade e segurança de seus ativos de informação.

O Gerente de Infraestrutura e Segurança trabalha juntamente com colaboradores da organização envolvidos em proteger os ativos de informação para aplicar as políticas definidas, identificar as áreas de atenção e implantar mudanças apropriadas de acordo com as necessidades. As responsabilidades especificas do Gerente de Infraestrutura e Segurança incluem:

Responsabilidades do Gerente de Infraestrutura e Segurança

- Tomar decisões de alto nível pertinentes às Políticas de Segurança da Informação e seu conteúdo. Aprovar, antecipadamente, exceções a estas políticas com base em análise caso-a-caso.
- Coordenar, anualmente, uma verificação de risco formal para identificar novas ameaças e vulnerabilidades e identificar controles apropriados para minimizar qualquer novo risco.
- Rever anualmente as políticas e procedimentos de segurança da informação para manter a adequação face às emergentes necessidades de negócio ou ameaças à segurança.
- Manter atualizado o Plano de Resposta a Incidentes conforme definido nesta política.
- Realizar as convocações para reuniões ordinárias do Comitê de Segurança de Informação.
- Completar as tarefas de acordo com os Procedimentos Periódicos de Segurança Operacional.
- Monitorar e analisar alertas de segurança e distribuir informações ao pessoal apropriado de segurança, técnico e da administração da unidade de negócios.
- Aplicação das políticas e procedimentos de segurança da informação de acordo com sua aplicabilidade a todos os ativos de informação.
- Administração das contas de usuários e gerenciamento de autenticação.

4.2.2 Premissa de Segurança da Informação

A proteção bem sucedida dos sistemas da organização requer que vários departamentos e grupos sigam consistentemente uma visão compartilhada de segurança.

O Comitê de Segurança da Informação trabalha com os gerentes, administradores e usuários de sistemas dos departamentos no desenvolvimento de políticas, normas e procedimentos de segurança para garantir a proteção dos ativos da organização.

O Comitê de Segurança da Informação possui a responsabilidade sobre o planejamento, a educação e a conscientização sobre o tema da segurança da informação. As responsabilidades específicas do Comitê de Segurança da Informação incluem:

Responsabilidades do Comitê de Segurança da Informação

- Criar novas políticas e procedimentos de segurança da informação quando necessário. Manter e atualizar políticas e procedimentos de segurança da informação existentes. Rever anualmente as políticas e auxiliar a administração com o processo de aprovação.
- Atuar pró-ativamente para implantação das políticas de Segurança da Informação.
- Criar e manter procedimentos de resposta a incidentes.
- Restringir e monitorar o acesso a áreas restritas e informação confidencial. Assegurar que os controles adequados estejam disponíveis onde houver informações confidenciais.

4.2.3 Departamento de Recursos Humanos

Devido ao seu relacionamento direto e constante com os funcionários, assim como sua posição única de ter a primeiras e últimas interações com todos os colaboradores, o Departamento de Recursos Humanos tem um papel importante no que se referem à segurança das informações dentro da organização, sendo os seguintes itens de sua responsabilidade:

Responsabilidades do Recursos Humanos

- Auxiliar o Comitê de Segurança da Informação com a publicação e divulgação das políticas de Segurança da Informação e orientação sobre o uso aceitável a todos os usuários de sistema relevantes incluindo prestadores de serviço.
- Trabalhar com o Comitê de Segurança da Informação na disseminação de informações de conscientização sobre segurança, utilizando diversos métodos de comunicação, de conscientização e educação dos funcionários (ex. pôsteres, cartas, memorandos, treinamento via web, reuniões, etc.).
- Trabalhar com o Comitê de Segurança da Informação para administrar sanções e ações disciplinares referentes a violações da Política de segurança da informação.
- Notificar o Departamento de Tecnologia da Informação quando qualquer funcionário for contratado ou desligado.

4.2.4 Departamento de Treinamentos

Devido à necessidade constante por capacitação e conscientização dos colaboradores, o Departamento de Treinamentos deve atuar realizando treinamentos conforme as responsabilidades descritas a seguir:

Responsabilidades do Departamento de Treinamentos

- Certificar–se de que os funcionários que são impactados e/ou lidam diretamente com os temas abordados nesta política recebam o treinamento adequado para execução de suas tarefas.
- Registrar os treinamentos realizados por meio de controles de presença.
- Desenvolver metodologias adequadas objetivando os resultados esperados dos treinamentos.
- Avaliar a eficácia dos treinamentos por meio de avaliações de satisfação dos colaboradores.

4.2.5 Usuários

Todos os usuários de recursos computacionais e de informação da organização devem estar cientes da importância fundamental de tais recursos e reconhecer sua responsabilidade pela manutenção segura dos mesmos. Os usuários devem protegê-los contra abusos que interrompam ou ameacem a viabilidade de todos os sistemas. As seguintes responsabilidades são específicas a todos os usuários de sistemas computacionais da organização:

Responsabilidades dos Usuários

- Entender as consequências de suas ações relacionadas às práticas de segurança computacional e agir de forma condizente. Aceitar a filosofia de que “Segurança é responsabilidade de todos" auxiliando a organização a garantir a preservação de seus ativos e sistemas.
- Manter-se cientes sobre o conteúdo das políticas de Segurança da Informação.
- Ler e assinar a o termo de confidencialidade das informações que lhes forem confiadas em razão de sua atividade profissional.
- Agir constantemente de forma a seguir as classificações de confidencialidade dos ativos de informação da organização, de acordo com a Política de Gestão de Ativos.

4.3. Segregação de Funções

Para todos os ambientes da organização, sejam eles de produção ou desenvolvimento, é obrigatória a implementação de segregação de funções. A segregação de funções determina que funções conflitantes e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação não autorizada, coibindo o mau uso dos ativos da organização intencional ou não intencionalmente. Para casos de exceção, seja por limitação técnica ou de negócio, é obrigatório o uso de controles adicionais de segurança e a aprovação do Gerente de Infraestrutura e Segurança.

4.4. Contato com as Autoridades Externas

Como parte do processo de comunicação interno e externo e do plano de resposta a incidentes de segurança da informação da organização, declara-se que qualquer comunicação relacionada à segurança da informação, junto às autoridades externas que incluem, mas não se limitam a entidades reguladoras, entidades de conformidade e governo, devem ser previamente autorizadas pela Diretoria.

4.5. Segurança da Informação no Gerenciamento de Projetos

Como parte da metodologia de gerenciamento de projetos da organização, recomenda-se que os projetos incluam a segurança da informação dentro do seu ciclo de vida. A inclusão tem como objetivo avaliar os riscos de segurança da informação, bem como propor controles adequados e acrescentar aos objetivos do projeto, aspectos de segurança de informação.

4.6. Conformidade Legal

Todos os ativos e sistemas de informação organização, assim como os seus funcionários e prestadores de serviço devem estar em conformidade com as obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação estabelecido pela organização.

Com objetivo de prevenir violações, todas as informações armazenadas ou que trafeguem dentro dos perímetros físicos e lógicos da organização podem ser monitoradas, mediante o processo de aprovação instituído, revisado pelo Comitê de Segurança da Informação. Violações não serão toleradas e as sanções apropriadas serão aplicadas.

5 Seções da Política de Segurança da Informação

5.1. Política de Gestão de Ativos

Todos os ativos físicos e de informação da organização deverão ser classificados de acordo com o seu nível de confidencialidade, disponibilidade, integridade e controles legais. Uma vez classificados, devem ser respectivamente relacionados ao modo como são acessados, armazenados, movimentados e por fim descartados. Para detalhes e informações adicionais, consulte a Política de Segurança da Informação - Gestão de Ativos.

5.2. Política de Controle de Acesso

Todos os sistemas de informação da organização devem estar integrados a um sistema de controle de acesso definido pelo Departamento de Tecnologia da Informação.

A concessão de acessos (recursos ou sistemas) devem ser aprovados pelo gestor da informação. Além disso, deve ser instituída a segregação de função de acordo com nível funcional ou responsabilidade assim como uma revisão periódica dos acessos concedidos, a fim de evitar acessos indevidos. Para mais informações, consulte a Política de Segurança da Informação - Controle de Acesso.

5.3. Política de Criptografia

Quando pertinente, as informações da organização ou de parceiros e clientes que precisem ser protegidas contra acesso não autorizado ou estabelecido por normas externas ou internas de conformidade devem ser criptografadas conforme os padrões alinhados e definidos entre o responsável pela informação e seu detentor, de modo a garantir sua a confidencialidade, autenticidade e integridade. Para mais informações, consulte a Política de Segurança da Informação - Criptografia.

5.4. Política de Segurança Física e do Ambiente

É necessário estabelecer o perímetro de segurança física de modo a preservar o acesso somente a pessoas autorizadas. Além disso, deve ser instituído de modo obrigatório o uso de identificação visual (crachá) para visitantes, clientes, fornecedores e prestadores de serviço. Para controle e liberação de acesso de colaboradores, deve-se utilizar sistema de registro de acesso físico por meio de sistemas de catracas, torniquetes e biometria. Para mais informações, consulte a Política de Segurança da Informação - Segurança Física e do Ambiente.

5.5. Política de Gestão de Operações

O Departamento de Tecnologia da Informação, conjuntamente com o Comitê de Segurança da Informação, deve estabelecer as diretrizes para garantir a operação segura e correta dos recursos de processamento da informação. Para isso deve estabelecer procedimentos operacionais documentados e acessíveis aos usuários necessários.

Estes procedimentos operacionais devem incluir e não se limitar a, procedimentos de instalação e configuração de sistemas, procedimentos para manipulação de informação, procedimentos de cópias de segurança (backup) e procedimentos para gerenciamento de falhas de produção.

Para mais informações, consulte a Política de Segurança da Informação - Segurança de Operações.

5.6. Política de Gestão de Mudanças

Deve ser estabelecido um processo único de gestão de mudanças com o objetivo de controlar e garantir a autorização e documentação de toda mudança no ambiente que possa impactar no fluxo de processos da organização. Para mais informações, consulte a Política de Segurança da Informação - Gestão de Mudanças.

5.7. Política de Segurança nas Comunicações

O Departamento de Tecnologia da Informação, conjuntamente com o Comitê de Segurança da Informação, deve estabelecer as diretrizes para garantir a proteção das informações em redes e dos recursos de processamento da informação que as apoiam. Para isso deve estabelecer procedimentos operacionais documentados e acessíveis aos usuários necessários, que estabeleçam as responsabilidades e procedimentos sobre o gerenciamento de equipamentos de rede. Para mais informações, consulte a Política de Segurança da Informação - Segurança nas Comunicações.

5.8. Política Gestão de Sistemas da Informação e Infraestrutura

Todos os processos que envolvam aquisição, desenvolvimento ou manutenção de sistemas de informação ou alteração na infraestrutura da organização devem ser comunicados ao Departamento de Tecnologia da Informação, garantindo que os riscos relacionados sejam conhecidos e tratados. Para mais informações, consulte a Política de Segurança da Informação - Gestão de Sistemas da Informação e Infraestrutura.

5.9. Política de Gestão de Incidentes de Segurança da Informação

O processo de gestão de incidentes de segurança da informação tem como objetivo garantir que eventos de segurança da informação associados a ativos de informação da organização sejam comunicados ao Departamento de Tecnologia da Informação.

É de responsabilidade do Departamento de Tecnologia da Informação coordenar todas as atividades pertinentes ao processo de gestão de incidentes de segurança da informação. É dever de todos os usuários comunicar um incidente de segurança da informação para área responsável. Para mais informações, consulte a Política de Segurança da Informação - Gestão de Incidentes.

6 Regulamentos Externos

ISO 27000

7 Anexos

- Política de Controle de Acesso
- Política de Criptografia
- Política de Gestão de Ativos
- Política de Gestão de Incidentes de Segurança da Informação

- Política de Gestão de Mudanças
- Política de Gestão de Operações
- Política de Segurança Física e do Ambiente
- Política de Segurança nas Comunicações
- Política de Sistemas de Informação e Infraestrutura

8 Histórico de Revisões

Abaixo se encontra a tabela com o histórico de revisões deste documento.

REVISÃO	ELABORADO POR	REVISADO POR	APROVADO POR	DATA DA APROVAÇÃO
2.0	Priscila/Monica	R. Polito/Marcelo	Ricardo Barros	03/05/2016
3.0	Daniel/Marcelo	R. Polito/Priscila	Ricardo Barros	09/10/2017

Este termo deve ser assinado e arquivado no prontuário do colaborador.

TERMO DE CIÊNCIA E COMPROMETIMENTO

Via da Empresa

Recebi o Manual PSI – Política de Segurança da Informação, cujo propósito é esclarecer a política da empresa e os padrões de comportamentos esperados de seus colaboradores.

Comprometo-me a cumpri-lo integralmente e dar ciência do não cumprimento por terceiros e em casos de dúvidas, consultar meus superiores ou o Comitê de Segurança da Informação.

Li e compreendi,

_____

Nome

_____

Assinatura do Colaborador

Local: Osasco, Data _____/_____/ 20___.

TERMO DE CIÊNCIA E COMPROMETIMENTO

Via do Colaborador

Recebi o Manual PSI – Política de Segurança da Informação, cujo propósito é esclarecer a política da empresa e os padrões de comportamentos esperados de seus colaboradores.

Comprometo-me a cumpri-lo integralmente e dar ciência do não cumprimento por terceiros e em casos de dúvidas, consultar meus superiores ou o Comitê de Segurança da Informação.

Li e compreendi,

_____

Nome

_____

Assinatura do Colaborador

Local: Osasco, Data _____/_____/ 20___.