POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

REVISÃO| 01 DATA| 31-05-2019

ÍNDICE

1. DISPOSIÇÕES GERAIS

OBJETIVO

Estabelecer as diretrizes que permitam aos colaboradores da S2 seguirem padrões de comportamento relacionados à Segurança da Informação, a fim de assegurar a confidencialidade, integridade e disponibilidade dos ativos da informação críticos para os negócios da Empresa, com o intuito de suportar sua operação, protegê-la de riscos, e assegurar o cumprimento de requisitos regulamentares, operacionais e contratuais.

ABRANGÊNCIA

Esta política aplica-se a todos os colaboradores da S2 Consultoria Empresarial Ltda.

VIGÊNCIA

Esta política entra em vigor na data de sua publicação.

2. DEFINIÇÕES

2.1 SEGURANÇA DA INFORMAÇÃO

A norma NBR ISSO/IEC 27002, define que a Segurança da Informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*.

Estes controles devem ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

Neste sentido, a Área de Segurança da atua nos seguintes campos:

a) Gestão de Acessos;

b) Continuidade de Negócios;

c) Segurança de Redes, Dados e Sistemas;

d) Gestão de Incidentes de Segurança;

e) Conscientização, sensibilização e Treinamento em Segurança;

f) Gestão de Riscos e Vulnerabilidades; e

g) Projetos de Segurança.

A Área de Segurança da Informação se utiliza de princípios básicos que tem o objetivo de proteger e suportar a operação da S2 e de fomentar o uso responsável quanto ao acesso e utilização da informação.

- ✓ Cumprir com requisitos legais e regulatórios;
- ✓ Avaliar ameaças atuais e futuras ao negócio;
- ✓ Proteger informações críticas;
- ✓ Desenvolver sistemas e Serviços com Segurança; e
- ✓ Agir de maneira profissional e ética.

Diante disto, manter a confidencialidade, integridade e disponibilidade da informação são essenciais para preservar a competitividade, faturamento, lucratividade, atendimento dos requisitos legais e a imagem da Empresa no mercado.

2.2 CONFIDENCIALIDADE

Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

2.3 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.

2.4 DISPONIBILIDADE

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

2.5 INFORMAÇÃO

A informação é um ativo essencial para os negócios da instituição e, por este motivo deve ser adequadamente protegida. A informação pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas.

3. INFORMAÇÃO

3.1 PROTEÇÃO À INFORMAÇÃO

Todo usuário possui responsabilidade das informações sob sua custódia e deve estar ciente de riscos que representa ao negócio, tais como, vazamento de informação e fraudes, devendo tomar cuidados quanto ao uso da informação.

Usuários devem se preocupar e ter cuidado com a exposição e descarte de documentos e mídias, por exemplo, ao expor informações em telas de computador, mesas de trabalho, salas de reunião, impressoras, conversas ao telefone, etc.

3.2 PROPRIEDADE DA INFORMAÇÃO

Qualquer informação proveniente de colaboradores, prestadores de serviços ou fornecedores que tenha sido criada e/ou que esteja armazenada em qualquer recurso da instituição é considerada propriedade da S2, não podendo ser tomada como de uso pessoal. Isto inclui, por exemplo, não se limitando a, e-mails, documentos, vídeos, cartazes, apresentações, fotos, etc.

3.3 PRIVACIDADE

Esse tópico está detalhado na "**Política Geral de Proteção de Dados Pessoais**".

3.4 ACESSO, MANIPULAÇÃO, USO E DESCARTE

Toda informação ou ativo da informação disponibilizado pela S2 deve ser utilizado para propósitos de negócio e finalidades aprovados pela Empresa, cabendo ao colaborador o seu uso correto e aceitável, na medida em que ele tem total responsabilidade das informações que estão em sua custódia.

3.5 MARKETING E PUBLICAÇÕES

Qualquer material destinado à publicação externa ou interna e material que utilize qualquer marca da S2 deve ser revisado pela Área de Marketing e, quando necessário, esta irá interagir e gerenciar todos os contatos com a mídia.

A utilização de qualquer marca da S2 deve ser autorizada pelos Sócios.

3.6 CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação de propriedade ou em custódia da S2 deverá ser classificada apropriadamente de acordo com sua confidencialidade, cabendo ao gestor notificar os colaboradores e prestadores, de suas responsabilidades de trabalho diante da propriedade intelectual, conforme os níveis abaixo:

- Confidencial;
- Restrito ou de Uso Interno;

- Público.

3.7 LIGAÇÕES

Todas as ligações são passíveis de auditoria sem aviso prévio, de forma a garantir sua existência e disponibilidade.

4. ACESSO LÓGICO

Tem como objetivo controlar com base nos requisitos de negócio da Empresa, os acessos e recursos de processamento das informações inerentes ao negócio. O acesso lógico é concedido baseado em desenho de perfis, de acordo com a função desempenhada por cada usuário da S2.

O uso de recursos tecnológicos e sistemas são concedidos para o uso profissional e de interesse exclusivo da empresa. É permitido o uso pessoal de alguns recursos, como Internet e e-mail, desde que não comprometa os recursos internos e que não infrinja as diretrizes estabelecidas nesta política.

Os acessos concedidos aos usuários devem ser revisados anualmente, sob demanda e sempre que houver suspeita de violação da segurança.

Cabe à Área de Segurança da Informação, quando da revisão anual dos acessos, demandar para os Gestores de Área responsáveis por perfis de acesso e para Gestores de Negócio responsáveis pela gestão de Sistemas e/ou Aplicações, a revisão dos acessos concedidos, e cabe a estes, solicitar à Área de Segurança da Informação, quando da necessidade de permanência, modificação ou remoção de acessos à Sistemas e/ou Aplicações concedidos aos usuários.

4.1 IDENTIFICAÇÃO ÚNICA (ID)

Todos os colaboradores, prestadores de serviços e estagiários devem possuir um *login* de acesso (ID) único e senha como identificação, sendo estes itens mandatórios para que se tenha acesso a qualquer ativo da informação e devem ser desabilitados durante o período de férias, licença, afastamento ou ao final do contrato de trabalho.

As informações e recursos correlacionados ao (ID) são de uso pessoal e intransferível, sendo o seu compartilhamento passível de penalizações administrativas.

Para prestadores de serviços a validade do ID de identificação é de no máximo de 3 meses, sendo necessária sua prorrogação, o gestor responsável deve, com antecedência, formalizar o pedido para a Área de Segurança da Informação.

4.2 ADMISSÃO

Nos processos de Admissão a área de Recursos Humanos deve comunicar às áreas da Empresa que atuam na liberação de recursos e acessos, para que sejam disponibilizados os recursos e acessos necessários para atuação do novo colaborador.

4.3 DEMISSÃO, FÉRIAS, LICENÇA E ALTERAÇÃO DE DEPARTAMENTO

Nos processos de Demissão, Férias, Licença e Alteração de Departamento, a área de Recursos Humanos deve emitir comunicado e mediante a este, para execução de procedimentos de revogação ou bloqueios dos acessos, conforme situação.

Quando do desligamento de um colaborador, imediato ao comunicado, deve-se bloquear os acessos.

No processo de alteração de departamento, deve-se readequar os acessos, de acordo com o novo perfil de acesso que o usuário deve possuir, bem como revogar os acessos advindos do cargo/departamento anterior.

Quando do gozo de férias, deve-se bloquear os acessos do colaborador durante o período informado pela Área de Recursos Humanos. Durante o período de férias.

4.4 CORREIO ELETRÔNICO

O Correio Eletrônico, e-mail, fornecido pela S2 aos funcionários ou prestadores de serviços, é uma ferramenta de trabalho e deve ser utilizado apenas para fins corporativos. Suas informações são de propriedade da S2 e são passíveis de auditoria sem aviso prévio, conforme critérios estabelecidos no item 3.3 desta Política. Desta forma não há privacidade ou sigilo para seu conteúdo.

Cada colaborador é responsável pelo conteúdo de textos ou equipamentos multimídias enviados por seu e-mail corporativo, devendo se preocupar, inclusive, com o envio de informações internas e sigilosas.

Estão vedadas práticas abusivas tais como: a circulação de spam, conteúdo discriminatório ou racista, material pornográfico, entre outros, cabendo sanções administrativas pelo descumprimento que podem chegar, inclusive, a dispensa por justa causa.

Está também vedado o envio de dados corporativos para fora da S2 sem as devidas autorizações ou justificativas do fim a que se destinam.

Colaboradores devem se valer de boas práticas quanto ao uso de e-mails, sobretudo tomando o cuidado de não usar linguagens impróprias, ofensivas, de baixo calão ou

discriminatórias, e de não enviar "correntes", mensagens de engajamento sobre qualquer atividade ilegal, imprópria ou não ética, mensagens de conotação sexual, religiosa ou política, mensagens de propaganda não relacionadas ao negócio da S2.

Além disto, é vedada qualquer comunicação em nome da S2 através de contas de e-mail particulares.

4.7 ACESSO AO DRIVE (NUVEM)

Todos os colaboradores têm direito de acesso ao drive do departamento no qual exerce as atividades inerentes à sua função.

Para Auditores Externos, Prestadores de Serviço e Consultores, a concessão de acesso ao drive deve ocorrer mediante aprovação do Gestor de Negócio responsável pelo diretório solicitado.

É proibida a guarda de arquivos não autorizados, bem como fazer uso das informações da S2.

É terminantemente proibido o armazenamento de material corporativo no disco local das máquinas (drive c:), em virtude do diretório drive c: não passar pelo processo de backup, diante disto a perda das informações é definitivo, não podendo ser recuperadas.

4.8 UTILIZAÇÃO SENHA CORPORATIVA E ATIVOS

As senhas de acesso corporativo são de uso pessoal, intransferível, cabendo ao seu titular total responsabilidade quanto a sua guarda.

Todo usuário deve seguir as melhores práticas quanto à criação, alteração e uso de senhas (devem ser alteradas a cada 60 dias), como, sendo inteiramente responsável por seu sigilo, devendo solicitar sua troca imediata quando suspeitar de seu comprometimento.

Compartilhar senhas de acesso é terminantemente proibido, cabendo sanções administrativas pelo descumprimento.

Os ativos sob a responsabilidade da S2 devem estar configurados com o bloqueio automático do sistema e devem solicitar uma nova autenticação após 5 minutos de inatividade da sessão.

4.9 SOFTWARES E SISTEMAS

Todos os Sistemas e *Softwares* utilizados pelo colaborador devem ser aprovados pela S2. É proibido a instalação de qualquer Sistema sem licença ou homologada pela

Empresa “Softwares Piratas” ou sem autorização de uso pela Área de Tecnologia/ Segurança da Informação.

Todos os sistemas corporativos devem ter um Gestor da Informação nomeado, além de todas as manutenções e/ou parametrizações realizadas nos sistemas aplicativos devem ser documentadas e formalmente aprovadas pelo Gestor da Informação.

Quando da realização de manutenções e/ou parametrizações nos sistemas, os testes formais de homologação de sistemas devem ser realizados por usuários chave de negócio, sendo de responsabilidade do Gestor da Informação a aprovação final da homologação.

Os ambientes (Aplicações e Servidores) de desenvolvimento, homologação e produção devem ser segregados. Fica restrito o acesso dos desenvolvedores ao ambiente de desenvolvimento. Os ambientes de Produção e Homologação, somente as Áreas de Negócio responsáveis pela aplicação e equipe de Segurança da Informação terão acesso nestes ambientes.

4.10 BACKUP DOS DADOS CORPORATIVOS

A S2 realiza *backups* rotineiros e testes periódicos de restauração de dados, visando salvaguardar os ativos de informação da instituição.

Todos os dados obtidos por meio da rotina de *backup* são armazenados em repositórios seguros, protegidos contra acesso não autorizado e armazenados em prédio distinto da localização dos servidores.

4.11 SISTEMAS DE BANCO DE DADOS CORPORATIVOS

Todos os sistemas de Banco de Dados devem ter administração centralizada, com acesso restrito.

A solicitação de liberação de acesso ao Banco de Dados deve ser analisada e aprovada pelas Áreas de Segurança da Informação e Tecnologia da Informação.

Todas as alterações realizadas em nossas bases de dados devem possuir trilha de auditoria habilitada, sendo proibido o envio de informações confidenciais sem autorização da Área de Segurança da Informação.

Os ambientes das Bases de Dados são segregados para desenvolvimento, homologação e produção, com revisão anual pela equipe de Segurança da Informação nas bases de dados ambientes de Produção, Homologação e Desenvolvimento.

Fica proibido o acesso de colaboradores da área de desenvolvimento nos ambientes de homologação e de produção.

5. DISPOSITIVO FÍSICO

5.1 DISPOSITIVOS DE ARMAZENAMENTO REMOVÍVEIS

Dispositivos de armazenamento removível, como por exemplo: pen drive, CD, DVD, HD externos e zip drives, só podem ser usados mediante a criptografia.

5.2 EQUIPAMENTOS PESSOAIS

Não é permitido aos colaboradores o uso de dispositivos pessoais, tais como Notebooks, Tablets e telefones celulares.

5.3 GESTÃO DE ATIVOS DA INFORMAÇÃO

Cabe ao Encarregado da Proteção de Dados (doravante, "DPO"), conforme descrito na **Política Geral de Proteção de Dados Pessoais**, assegurar que estes seguem as melhores práticas relacionadas à proteção da confidencialidade, integridade e disponibilidade das informações.

Ativos tecnológicos devem possuir mecanismos que permitam a identificação, autenticação, autorização, controle de acessos e registro de atividades de usuários. Equipamentos e sistemas devem seguir melhores práticas quando à entrada, processamento, armazenamento e saída de informações.

Do mesmo modo, gestores devem assegurar que serviços, processos e pessoas, sob sua responsabilidade estão cientes e seguem as recomendações e diretrizes de segurança quanto às informações pelas quais tem acesso através dos dispositivos físicos disponibilizados pela S2.

6. INVESTIGAÇÃO E MONITORAMENTO DE CONDUTA

A Área de Segurança da Informação da S2 tem o direito de examinar qualquer ativo de informação de propriedade da Empresa, sem prévio consentimento, se houver suspeita de que algum desses ativos estejam sendo utilizados de forma indevida ou para fins não autorizados.

Somente pessoa autorizada pelos sócios da S2 pode implementar mecanismos para coletar senhas ou autenticar a identidade dos usuários, porém a gestão e análise das informações ficam restritas a equipe de Segurança da Informação.

7. COMPLIANCE

7.1 IDENTIFICAÇÃO DA LEGISLAÇÃO VIGENTE

Todos os sistemas aplicativos que atendam a estatutos, regulamentações ou cláusulas contratuais devem possuir esses requisitos explicitamente definidos e documentados.

Controles e responsabilidades específicos para atender a este requisito devem estar formalmente definidos.

7.2 VIOLAÇÃO DE DIREITOS AUTORAIS

É proibido o uso de *software* sem que haja autorização expressa em contratos de licenças de software, mesmo que a título oneroso, ou previstos em leis e regulamentações aplicáveis.

7.3 PROPRIEDADE INTELECTUAL

Toda propriedade intelectual deve ser identificada e classificada apropriadamente, cabendo ao gestor da área notificar os colaboradores de suas responsabilidades de trabalho diante da propriedade intelectual.

7.4 INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

A Área de Segurança da Informação é responsável pela apuração dos incidentes que envolvam a Confidencialidade, Integridade e Disponibilidade da informação, cabendo somente a ela à averiguação de possíveis vulnerabilidades e detalhes do incidente, exceto quando, previamente, autorizar que outros o façam.

Qualquer incidente de segurança deverá ser reportado para o DPO, conforme descrito na **Política Geral de Proteção de Dados Pessoais**, não devendo ser divulgados a terceiros ou outras partes que não estejam diretamente envolvidas com o incidente. Caberá ao DPO avaliar a necessidade de reporte de incidentes de segurança da informação para órgãos externos.

7.5 VIOLAÇÕES DA POLÍTICA

Qualquer violação às políticas de Segurança da Informação poderá implicar em penalidades administrativas e penalidades legais, não obstante, podendo implicar em sanções civis e criminais.

É obrigação de todo colaborador informar sobre violações desta política à Área de *Compliance*. A omissão poderá implicar em penalidades administrativas.

8. PAPÉIS E RESPONSABILIDADES

Todo colaborador é responsável pelo uso adequado de equipamentos e recursos tecnológicos sob seu controle, devendo utilizá-los para fins profissionais.

Todos os colaboradores, prestadores de serviços e fornecedores devem ser informados em relação ao conhecimento e à adoção das medidas de segurança da informação definidas pela S2, bem como suas responsabilidades na aderência e manutenção da segurança corporativa, de modo a evitar a ocorrência de incidentes de segurança.

8.1 DIRETORIA

a) Assegurar o cumprimento desta Política.

8.2 GESTORES

a) Garantir que colaboradores e terceiros tenham conhecimento desta política, assegurando a assinatura dos termos de confidencialidade e responsabilidade por colaboradores e prestadores de serviço;

b) Avaliar pedidos de autorização de acesso a sistemas e recursos por colaboradores e terceiros sob sua gestão;

c) Solicitar, a cada 03 (três) meses, a renovação dos acessos de terceiros e prestadores de serviços sob sua gestão, se aplicável;

d) Classificar e categorizar informações sob sua responsabilidade, de acordo com sua importância e confidencialidade;

e) Assegurar que os ativos da informação sob sua responsabilidade estão gerando informações íntegras e confiáveis;

f) Avaliar solicitações de acesso a sistemas sob sua gestão; e

g) Avaliar e revisar periodicamente, os usuários que possuem autorização de acesso a ativos da informação sob sua responsabilidade, solicitando cancelamento de autorizações quando aplicável.

8.3 USUÁRIO

a) Cumprir as diretrizes estabelecidas nesta Política, zelando pela proteção da informação, respeitando seu sigilo e seguindo o modelo de confidencialidade previamente classificado;

b) Uso adequado de equipamentos e recursos tecnológicos sob seu controle, sendo responsável por salvaguardar os ativos de informação;

c) Utilizar os recursos tecnológicos e sistemas corporativos somente para exercer suas funções de trabalho com autorização do seu gestor.

8.4 ENCARREGADO DA PROTEÇÃO DE DADOS

a) Deve realizar a guarda e manutenção das informações, sendo ela apresentada, por exemplo, contratos de operações, contratos de fornecedores, arquivos, e-mails etc;

b) Realizar *backups* da informação de forma a garantir sua existência e disponibilidade;

c) Apurar e reportar violações a esta Política; e

d) Reportar incidentes de segurança da informação à órgãos externos, quando aplicável.

8.5 ÁREA DE TECNOLOGIA DA INFORMAÇÃO

a) Gerir ativos da informação sob sua custódia, assegurando o cumprimento de políticas, normas e procedimentos aplicáveis;

b) Assegurar que os ativos da informação seguem as melhores práticas de segurança quanto à entrada, processamento, armazenamento e saída de informações; e

c) Não instalar *softwares* e sistemas que estejam em desacordo com as políticas e normas da S2.

8.6 ÁREA DE SEGURANÇA DA INFORMAÇÃO

a) Verificar se os controles existentes estão em conformidade com esta e demais Políticas de Segurança da Informação;

b) Avaliar Riscos e Vulnerabilidades em Processos e Sistemas da Informação;

c) Revisar os acessos concedidos a cada 12 (doze) meses ou sob demanda do Gestor de Negócio;

d) Executar a gestão dos acessos a sistemas corporativos, concedendo, alterando e removendo acessos quando necessário ou quando entendido que estes representam riscos a operação ou imagem da S2;

e) Desenhar, implantar e/ou demandar controles necessários para Processos, Sistemas e Operações da S2; e

f) Avaliar exceções a esta política.

8.7 ÁREA JURÍDICA

a) Incluir na análise e elaboração de contratos, sempre que necessário, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses da S2;

b) Aprovar em conjunto com Área de Marketing, o uso de qualquer marca do Grupo S2; e

c) Avaliar, quando solicitado, a política, as normas e procedimentos de segurança da S2.

8.8 ÁREA DE MARKETING

a) Revisar e aprovar qualquer publicação interna ou externa e material que utilize a marca da S2;

b) Responder dúvidas e questionamentos a respeito de assuntos institucionais e estratégicos que envolvam a marca do Grupo S2; e

c) Aprovar, em conjunto com Área Jurídica, o uso de qualquer marca do Grupo S2.

9. CONSENTIMENTO

O colaborador e/ou fornecedor, ao tomar ciência da política de segurança da informação, entende e concorda com as informações dispostas no documento, assim como as obrigatoriedades descritas.

Ainda, entende e concorda que toda e qualquer dúvida foi esclarecida para o cumprimento integral dos itens definidos pela política de segurança da informação.