OBJETIVO

A Política de Segurança da Informação estabelece as diretrizes, definidas e adotadas pelo Insper, em relação ao manuseio de dados e informações, bem como o tratamento que deve ser dado às informações armazenadas, processadas ou transmitidas tanto no ambiente convencional quanto no ambiente tecnológico.

A Diretoria está comprometida e apoia as diretrizes estabelecidas nesta Política bem como na proteção dos ativos tangíveis e intangíveis do Insper de acordo com as necessidades de negócio e em conformidade legal, garantindo a sua confidencialidade, integridade, disponibilidade, autenticidade e legalidade no tratamento das informações.

As orientações descritas neste documento são princípios fundamentais e representam como o Insper exige que as informações sejam utilizadas.

ABRANGÊNCIA

Esta política abrange:

a. Toda informação de propriedade ou sob responsabilidade do Insper;

b. O ambiente de informação digital;

c. O ambiente de informação convencional;

d. Todos os colaboradores do Insper;

e. Todas as áreas organizacionais do Insper.

DIRETRIZES

Esta política se aplica a todos os colaboradores do Insper, estagiários, trainees, fornecedores, clientes e terceiros vinculados a empresa que a qualquer momento tenham necessidade de acesso à informação.

Esta política e seus documentos complementares devem ser divulgados pela Área Responsável, visando dar publicidade para todos que se relacionam profissionalmente com o Insper.

TERMOS E DEFINIÇÕES

Informação: É um ativo que, como qualquer outro ativo importante para os negócios, tem valor para a organização e consequentemente necessita ser adequadamente protegido;

Usuário: Todos aqueles que utilizam os recursos de tecnologia da informação ou convencional, sendo, portanto, responsáveis pelo conhecimento e aplicação desta política, abrangendo os colaboradores do Insper, estagiários, temporários e terceiros vinculados a empresa;

Confidencialidade: É a garantia de que a informação é acessível somente por pessoas autorizadas;

Disponibilidade: É a garantia de que os usuários autorizados obtenham acesso à informação sempre que necessário;

Integridade: É a garantia da exatidão e confiabilidade da informação e dos métodos de processamento;

Incidente: Qualquer situação que possa afetar a confidencialidade, disponibilidade, ou integridade das informações do Insper e recursos de TI (ex: falha de sistemas ou rede, violação de acessos, infecção por vírus, ataque de hackers, incêndio, inundação etc..);

Usuário Patrono: Usuário responsável pelas funcionalidades de um ou mais sistemas do Insper, a quem cabe a aprovação prévia de melhorias a serem efetuadas no(s) sistema(s) de sua responsabilidade, bem como pela classificação, definição do perfil do usuário e do tipo de acesso às informações;

Acesso privilegiado: Também conhecido como acesso administrativo ou super-usuário. É definido como um acesso ampliado ou especial para recursos de TI dada aos operadores e administradores de sistema;

Trilha de Auditoria: É uma coleção de arquivos de log que contêm informações sobre as interações feitas nos sistemas onde é ativado;

Backup: Salvaguarda de informações, realizada por meio de reprodução e/ou espelhamento de uma base de arquivos, com a finalidade de plena capacidade de recuperação em caso de incidente ou necessidade de restore, ou ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada do Insper;

Dispositivos Removíveis de Armazenamento de Informação: Dispositivos capazes de armazenar informações que pode ser removida do equipamento, possibilitando a portabilidade dos dados, como CD, DVD e pen drive;

Violação: Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos do Insper;

RESPONSABILIDADES

Usuário: São responsáveis pela segurança das informações e tendo conhecimento de algum incidente relacionado, deverão reportar a Segurança da informação;

Segurança da Informação: Responsável pelos procedimentos, ações, instruções e normativos que possibilitem a operacionalização e manutenção desta política;

Diretoria: Analisar, aprovar e declarar formalmente o seu comprometimento com esta política. Aprovar os investimentos em segurança da informação no Insper, considerando a viabilidade e os impactos de sua aplicação à qualidade dos processos de negócio. Analisar e aprovar, ou não, as exceções de forma excepcional a essa política;

Auditoria Interna: Verificar o cumprimento e eficácia desta política, podendo solicitar sem aprovação prévia, observando as restrições legais aplicáveis, qualquer informação pertinente para a realização de auditorias ou outras apurações;

Departamento de Tecnologia da Informação: Garantir que todos os ativos tecnológicos atendam e suportem as diretrizes descritas nesta política. Auxiliar na análise dos incidentes de segurança da informação reportados;

Gestor da Informação: Responsável pela classificação das informações, autorização de acesso, validação de uso e definição dos demais controles sobre a informação;

Gestores: Assegurar e gerenciar o cumprimento desta política e demais documentos complementares pelos Colaboradores de sua equipe;

1. PLANEJAMENTO

A Segurança da Informação deve ser preocupação de todos e não apenas do Departamento de Tecnologia da informação e Segurança da Informação. Da mesma forma, deve refletir em hábitos, posturas, responsabilidades e cuidados constantes nos momentos de uso, solicitação e aprovação de recursos.

A Gerência de Tecnologia da informação em conjunto com a Segurança da informação providenciarão os recursos humanos e materiais necessários para implementação das diretrizes estabelecidas nesta Política, bem como orientar todos os usuários quanto às ações que serão tomadas, além de divulgar os

preceitos de segurança em tecnologia de informação a serem observados por todos, inclusive, nas unidades do Insper que possuam ambiente de TI distinto, com maior ou menor integração com o restante da organização.

A utilização das informações e dos recursos computacionais deve ser sempre compatível com a ética, confidencialidade e a finalidade das atividades desempenhadas pelo usuário.

A utilização de recursos (sistemas, correio eletrônico, espaço em disco, equipamentos etc.), disponibilizados pelo Insper, deve ser feita segundo os padrões e procedimentos definidos pelo Departamento de Tecnologia da Informação, visando manter a disponibilidade e o desempenho das aplicações.

A conexão de equipamentos de terceiros na rede do Insper somente será permitida com prévia aprovação do Departamento de Segurança da Informação, se não apresentar risco ao ambiente corporativo e estiverem de acordo com as políticas do Insper aplicáveis aos demais equipamentos.

A utilização indevida dos recursos computacionais, além das penalidades, pode provocar a suspensão dos acessos.

Qualquer violação desta política constitui base para uma medida disciplinar, inclusive o término do contrato empregatício, bem como às sanções previstas em lei.

1.1. Gestão de Ativos

Somente será permitido o uso de recursos homologados e autorizados pela empresa, desde que sejam identificados individualmente, inventariados, com documentação atualizada e atendendo a legislação pertinente em vigor.

A utilização destes, sem licenças correspondentes, é crime previsto na Lei 9.609, de 19 de fevereiro de 1998. Portanto, qualquer usuário que exponha a empresa a sanções jurídicas por utilização de softwares não homologados, independentemente de sua classificação (shareware, freeware, demo etc.) sem respaldo das respectivas licenças, está sujeito às medidas disciplinares internas e as previstas em lei.

1.1.1. Ativo Informação

Todos ativos devem ser protegidos, cuidados e gerenciados adequadamente com o objetivo de garantir a sua disponibilidade, integridade e confidencialidade, independentemente do meio de

armazenamento, processamento ou transmissão que esteja sendo utilizado.

Cada informação e ativo terá seu gestor que será indicado formalmente pela diretoria responsável pelos sistemas que acessam a informação.

1.1.2. Classificação da Informação

As informações classificadas como confidenciais e/ou reservadas requerem alto grau de controle e proteção contra acessos não autorizados, como também, aquelas que necessitam de sigilo por força de lei ou contrato são candidatas naturais à obtenção desta classificação.

Todas as Informações, que não forem explicitamente classificadas, devem ser tratadas como informações de Uso Interno.

As informações normalmente são classificadas, em uma das categorias a seguir, pelos seus respectivos gestores:

Confidencial: Informação de importância estratégica para o sucesso e continuidade dos objetivos do Insper, até que se tornem públicas. Se estiver indisponível, corrompida ou for acessada indevidamente pode acarretar severos incidentes financeiros, de reputação ao negócio ou de imagem, podendo levar à perda de diferencial competitivo. O seu manuseio é restrito a usuários previamente autorizados;

Uso Interno: Informação destinada à utilização interna por colaboradores e prestadores de serviço do Insper;

Pública: Informação que pode ser distribuída ao público externo, o que, usualmente, é feito através dos canais corporativos apropriados.

1.2 Proteção da Informação

Toda informação do Insper deve ser protegida para que não seja alterada, acessada e destruída indevidamente.

Os locais onde se encontram os recursos de informação devem ter proteção e controle de acesso físico compatível com o seu nível de criticidade.

1.3 Gerenciamento das operações

1.3.1 Gestão de mudanças

Todas as modificações nos recursos de TI, seja ele hardware ou software deverão ser registradas, tratadas, comunicadas e controladas somente pelo Departamento de Tecnologia da Informação.

1.3.2 Segregação de Ambiente e Funções

O Departamento de Segurança da Informação deve assegurar que todos os sistemas de informação do Insper sejam aderentes às diretrizes a seguir:

• Segregação de ambientes lógicos, de maneira que o ambiente de produção fique segregado dos demais;
• Os ambientes de teste, homologação e outros, devem ser de acesso exclusivo dos usuários envolvidos com atividades de desenvolvimento e suporte a sistemas;
• Usuários desenvolvedores deverão ter acesso apenas de consulta nos ambientes de produção;
• Todo objeto, tais como programas, telas, funções etc., que for transferido para o ambiente de produção, deverá ser originado do ambiente de desenvolvimento ou de homologação, mantendo nesses ambientes a fonte original.

1.3.3 Utilização da Informação e Recursos

Para acessar uma informação o usuário deve ser previamente autorizado. A autorização de acesso às informações será dada pelo Gestor da Informação. O acesso da informação deve ser autorizado apenas aos usuários que necessitam da mesma para o desempenho das suas atividades profissionais para o Insper. Qualquer tentativa de acesso consciente a ambientes não autorizados sofrerá medidas disciplinares.

O acesso da informação armazenada e processada no ambiente de TI é individual e intransferível. Este acesso acontece através da identificação e autenticação do usuário.

Os dados para autenticação do usuário devem ser mantidos em segredo e possuem o mais alto nível de classificação da informação. Os recursos de tecnologia da organização disponibilizados para os usuários têm como objetivo a realização de atividades profissionais.

As autorizações de acesso às informações devem levar em conta o perfil e as funções dos usuários. O Departamento de Segurança da Informação estabelecerá perfis de acesso dos usuários baseados nos requisitos de negócio do Insper.

1.3.4 Segurança de Acessos

A Segurança da Informação deve assegurar que cada usuário tenha uma única conta de acesso que seja pessoal e intransferível.

A conta de acesso de cada usuário é única, individual e intransferível, sendo reconhecidas como equivalentes à sua assinatura e representam nível de delegação concedida para o desempenho de suas funções.

A senha deve possuir um mínimo de 8 caracteres, contendo dígitos numéricos, alfabéticos e caracteres especiais. Nunca devem ser nulas ou estar em branco, nunca devem estar visíveis na tela onde são informadas e deverão ser bloqueadas após 3 tentativas consecutivas e mal sucedidas de acesso.

É proibido o compartilhamento de senhas entre os usuários. Qualquer identificação de compartilhamento de senha por parte dos usuários, ambos sofrerão medidas disciplinares.

Os acessos externos a recursos da empresa (acesso remoto de colaboradores, terceiros, fornecedores, clientes e outros casos que vierem a surgir) somente serão concedidos mediante autorização prévia da Segurança da Informação, segundo instruções detalhadas caso a caso e realizadas por intermédio de soluções técnicas corporativas.

Eventuais interligações entre redes (de forma física e/ou lógica) envolvendo processos de automação e/ou informação só serão permitidas utilizando soluções corporativas definidas pelo Departamento de Tecnologia da Informação aprovada pela Segurança da Informação, de forma a garantir a disponibilidade, a integridade e a confidencialidade dos ambientes.

1.3.5 Computação pessoal e móvel

O uso de mídias removíveis (HD Externo, Pen Drive, cartões de memória) nos equipamentos de TI do Insper serão previamente autorizados a cada usuário pela Segurança da Informação.

É proibido a conexão de equipamentos pessoais (Smartphones, Tablets e Notebooks) no ambiente de TI do Insper.

Os acessos a informações através de equipamentos móveis se darão através de equipamentos fornecidos pelo Insper.

1.3.6 Correio Eletrônico

As mensagens do correio eletrônico, disponibilizado para os usuários, obrigatoriamente devem ser escritas em linguagem profissional e que não comprometa a imagem da organização, não vá de encontro à legislação vigente e nem aos princípios éticos da organização. Cada usuário é responsável pela conta de correio eletrônico que lhe foi disponibilizado pelo Insper.

O conteúdo do correio eletrônico de cada usuário pode ser acessado e monitorado pela organização quando em situações que ponham em risco a sua imagem, seu negócio ou sua lucratividade. O usuário não deve ter expectativa de sigilo da sua conta de correio eletrônico disponibilizada pela organização para seu uso profissional.

1.3.7 Ambiente de Internet

O ambiente de Internet deve ser usado exclusivamente para o desempenho das atividades profissionais do usuário a serviço do Insper. Sites que não contenham informações que agreguem conhecimento profissional e para o negócio não devem ser acessados.

Os acessos realizados nesse ambiente são monitorados pela organização com o objetivo de garantir o cumprimento dessa política. O acesso à Internet é permitido somente por intermédio do sistema de segurança corporativo.

É proibido o acesso direto à Internet por intermédio de provedores externos estando conectado à rede corporativa.

1.4 Gestão de incidentes

Nenhum usuário deverá tomar ação própria sobre eventuais ocorrências de Segurança da Informação. Todos os usuários devem relatar à Linha Ética os eventos relacionados nesta política.

São considerados incidentes de Segurança da informação, mas não se limitando a estes:

- Perda de serviço, equipamento ou recurso;
- Erros humanos;
- Violações de procedimentos de segurança física;
- Mudança descontroladas dos sistemas;
- Vazamento de Informações;
- Violação de acesso.

1.5 Gestão da continuidade de negócio

Para enfrentar situações de interrupção dos sistemas de informação, com consequente paralisação das atividades de negócio, o Insper deverá manter um plano de contingência que permita operar os sistemas e recursos críticos de forma que garanta um nível mínimo de operação. O plano de contingência aprovado deverá ser exercitado com sucesso pelo menos uma vez ao ano.

Todos os procedimentos que possibilitam a proteção da informação e a continuidade do seu uso devem ser documentados, de tal forma que possibilite que o Insper continue a operacionalização desses procedimentos, mesmo na ausência do usuário responsável.

A definição e implementação das medidas de prevenção e recuperação, para situações de desastre e contingência, devem ser efetuadas de forma permanente e devem contemplar recursos de tecnologia, humanos e de infraestrutura. Elas são de responsabilidade da diretoria gestora dos recursos, contando com o apoio de validação do Departamento de Segurança da Informação.

Todas as informações críticas reportadas na análise de riscos utilizada para o funcionamento do Insper devem possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com proteção equivalente ao local principal. Esta informação deve ser suficiente para planos de continuidade de negócios.

A criação das cópias de segurança deve considerar os aspectos legais, históricos, de auditoria e de recuperação do ambiente.

1.6 Considerações Finais

A Segurança da Informação deve ser entendida como parte fundamental da política do Insper. Qualquer incidente pode de alguma forma comprometer o Insper e seus objetivos de negócio.

O não cumprimento de qualquer item desta instrução caracteriza uso indevido de informações ou de recursos de TI, e é considerado como violação de contrato, o assunto, de acordo com a sua gravidade, sofrerá sanções administrativas e judiciais adequadas.

O Insper se reserva ao direito de revisar, adicionar ou modificar essa Política de Segurança da Informação para aprimorar e garantir o perfeito funcionamento das normas e regras por ele definidas.