PSI | POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DIRETRIZES PARA A UTILIZAÇÃO
DOS RECURSOS DE
TECNOLOGIA E INFORMAÇÃO

2022

iTeam
fazendo diferente

Sumário

1. Objetivo 3
2. Termos e Definições 3
3. Escopo 8
4. Diretrizes 9
4.1. Geral 9
4.2. Ativos da Informação 9
4.3. Controle de Acesso 9
4.4. Controle de Acesso Físico 9
4.5. Controle de Acesso Lógico 10
4.6. Uso de Dispositivos Móveis 11
4.7. Segurança nas comunicações 14
4.8. Segurança com Fornecedores 15
4.9. Segurança em visitas de Fornecedores 15
4.10. Conformidades 15
4.11. Gestão de Incidentes de Segurança da Informação 15
4.12. Gestão da Continuidade de Negócio 15
4.13. Gestão de Melhoria Contínua 15
5. Responsabilidades 16
5.1. Usuários 16
5.2. Gestor 17
5.3. Equipe do SGPI 17
5.4. Área de Recursos Humanos 17
6. Documentos relacionados 17
7. Alterações da Política de Segurança da Informação 17

1. Objetivo

Em nosso processo de aperfeiçoamento contínuo, suportado por uma decisão estratégica de nossa alta direção, desenvolvemos um Sistema de Gestão de Privacidade da Informação (SGPI - sistema de gestão da segurança da informação que considera a proteção da privacidade como potencialmente afetada pelo tratamento de DP), normatizado, que visa a adoção de normas e procedimentos relacionados à segurança da informação permitindo aos colaboradores e demais partes interessadas seguir um padrão de comportamento relacionados a proteção da informação. Consideramos que através da observância dos 4 (quatro) pilares da segurança da informação, confidencialidade, integridade, disponibilidade e conformidade podemos atender às necessidades dos nossos clientes e do nosso mercado de atuação, além de assegurar que a nossa imagem de fornecedor de produtos e serviços de alta qualidade seja mantida e continuamente aprimorada.

2. Termos e Definições

- **Disponibilidade**: Os sistemas e os dados devem estar disponíveis de forma que quando o usuário necessitar, possa usar.
- **Integridade**: Os sistemas e os dados devem estar sempre íntegros e em condições de serem utilizados; Propriedade de salvaguarda da exatidão e completeza dos ativos.
- **Confidencialidade**: Os dados privados devem ser apresentados somente aos donos ou a pessoas ou grupo por eles liberados; Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.
- **Autenticidade**: Os sistemas e os dados devem ter condições de verificar a identidade dos usuários, e este ter condições de analisar a identidade do sistema; Propriedade que uma entidade é o que afirma ser.
- **Eficácia**: Extensão na qual as atividades planejadas são realizadas e os resultados planejados, alcançados.
- **Eficiência**: Relação entre o resultado alcançado e os recursos usados.
- **Fornecedor**: Qualquer organização que forneça bens e serviços. A utilização desses bens e serviços pode ocorrer em qualquer estágio de projeto, produção e utilização dos produtos. Assim, fornecedores podem incluir distribuidores, revendedores, prestadores de serviços terceirizados, transportadores, contratados e franquias, bem como os que suprem a organização com materiais e componentes. São também fornecedores os prestadores de serviços da área de saúde, treinamento e educação.

- **Partes Interessadas**: Um indivíduo ou um grupo de indivíduos com interesse comum no desempenho da organização e no ambiente em que opera. A maioria das organizações possui as seguintes partes interessadas: os clientes, a força de trabalho, os proprietários, os fornecedores, os parceiros de negócio e a sociedade. A quantidade e a denominação das partes interessadas podem variar em função do perfil da organização.
- **Produto**: Resultado de atividades ou processos. Considerar que:
  - O termo produto pode incluir serviços, materiais e equipamentos, informações ou uma combinação desses elementos;
  - Um produto pode ser tangível (como, por exemplo, equipamentos ou materiais) ou intangível (por exemplo, conhecimento ou conceitos), ou uma combinação dos dois; e
  - Um produto pode ser intencional (por exemplo, oferta a clientes), ou não-intencional (por exemplo, um poluente ou efeitos indesejáveis).
- **Qualidade**: Grau no qual um conjunto de características inerentes (atividade ou um processo, um produto, uma organização ou uma combinação destes), satisfaz os requisitos explícitos e implícitos dos clientes.
- **Requisito**: Necessidade ou expectativa que é expressa, geralmente, de forma implícita ou obrigatória.
- **Conformidade**: Atendimento a um requisito.
- **Não-conformidade**: Não atendimento a um requisito.
- **Gestão da segurança e privacidade da informação**: Conjunto de elementos inter-relacionados ou interativos para controlar e dirigir uma organização no que diz respeito à segurança da informação e proteção de dados pessoais.
- **Materiais e Serviços**: Materiais ou serviços que impactam na qualidade do produto.
- **Indeterminado**: Aquilo que não está definido. O tempo de retenção para os registros do nosso SGPI que estão definidos como indeterminado em função do seu arquivamento em meio eletrônico.
- **Projeto**: Significa o desenho de uma solução, sistema ou produto.
- **Controle de acesso**: Meios para assegurar que o acesso a ativos é autorizado e restrito com base nos requisitos de segurança e de negócios.
- **Responsabilidade**: Responsabilidade de uma entidade para suas ações e decisões.
- **Ativo da Informação**: Qualquer coisa que informação que agregue valor para a organização.
  - *NOTA: Existem vários tipos de ativos, incluindo:*
    - *a) informações;*
    - *b) software, como um programa de computador;*
    - *c) físicos, tais como o computador;*
    - *d) serviços;*
    - *e) pessoas e suas qualificações, competências e experiência; e*
    - *f) intangíveis, como reputação e imagem*

- **Ataque**: Tentativa que para destruir, expor, alterar, desabilitar, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um ativo.
- **Disponibilidade**: Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.
- **Continuidade do negócio**: Processo e/ou procedimento para garantir a contínua operações de negócio
- **Controle**: Meios de gerenciamento de risco, incluindo políticas, procedimentos, guias, práticas ou estruturas organizacionais, que podem ser administrativas, técnica, de gestão ou de natureza legal.
- **Objetivo de controle**: Declaração descrevendo o que é para ser alcançado como resultado da implementação de controles.
- **Ação Corretiva**: Ação para eliminar a causa de uma não-conformidade identificada ou outra situação indesejável.
- **Eficácia**: Extensão na qual as atividades planejadas são realizadas e os resultados planejado alcançados.
- **Eficiência**: Relação entre o resultado alcançado e os recursos usados.
- **Evento**: Ocorrência de um determinado conjunto de circunstâncias.
- **Guia**: Recomendação de que deverá ser feito para alcançar um objetivo.
- **Impacto**: Mudança adversa ao nível dos objetivos de negócios alcançado.
- **Ativo da informação**: Conhecimento ou dados que tem valor para a organização.
- **Segurança da informação**: Preservação da confidencialidade, integridade e disponibilidade da informação;
    - *NOTA: adicionalmente, outras propriedades, tais como a autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.*
- **Evento de segurança da informaçã**o: Uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.
- **Incidente de segurança da informação**: Um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.
- **Sistema de Gestão da Privacidade da Informação – SGPI**: A parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação e proteção de dados pessoais.
- **Risco de segurança da Informação:** Potencial que uma ameaça irá explorar uma vulnerabilidade de um ativo ou grupo de ativos e, assim, causar danos à organização.
- **Sistema de gestão**: Estrutura de políticas, procedimentos, guias e recursos associados, para atingir os objetivos da organização.

- **Não-repúdio**: Capacidade de provar a ocorrência de um evento alegado ou de ação e de suas entidades de origem, a fim de resolver disputas sobre a ocorrência ou não ocorrência de evento ou ação e envolvimento de entidades no evento.
- **Política**: Intenção e direção como formalmente expressado pela alta direção.
- **Procedimento**: Forma especificada de executar uma atividade ou um processo.
- **Processo**: Conjunto de atividades inter-relacionadas ou interativas que transformam insumos (entradas) em produtos (saídas).
- **Registro**: Documento que apresenta resultados obtidos ou fornece evidências de atividades realizadas.
- **Confiabilidade**: Propriedades de comportamento desejado consistente e os resultados.
- **Risco**: Combinação da probabilidade de um evento e suas consequências.
- **Aceitação de risco**: Decisão de aceitar um risco.
- **Avaliação de risco**: Todo o processo de análise de risco e avaliação de riscos.
- **Comunicação de risco**: Troca ou compartilhamento de informações sobre riscos entre o tomador de decisões e outras partes interessadas.
- **Critérios de risco**: Termos de referência pelo qual é avaliada a importância do risco.
- **Estimativa dos riscos**: Atividade para atribuir valores a probabilidade e consequências de um risco.
- **Avaliação de riscos**: Processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.
- **Gestão de riscos**: Atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos.
- **Tratamento do risco**: Processo de seleção e implementação de medidas para modificar um risco.
    - *Nota: Nesta Norma o termo "controle" é usado como um sinônimo de "medida".*
- **Declaração de aplicabilidade**: Declaração documentada que descreve os objetivos de controle e controles que são pertinentes e aplicáveis ao SGPI da organização.
    - *Nota: Os objetivos de controle e controles estão baseados nos resultados e conclusões dos processos de análise/avaliação de riscos e tratamento de risco, dos requisitos legais ou regulamentares, obrigações contratuais e os requisitos de negócio da organização para a segurança da informação.*
- **Ameaça**: Causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização.
- **Vulnerabilidade**: Fraqueza de um ativo ou controle que pode ser explorada por uma ameaça.
- **Risco residual**: Risco remanescente após o tratamento de riscos.
- **Aceitação do risco**: Decisão de aceitar um risco.
- **Análise de riscos**: Uso sistemático de informações para identificar fontes e estimar o risco.

- **Análise/avaliação de riscos**: Processo completo de análise e avaliação de riscos.
- **Mitigação**: Limitação das consequências negativas de um determinado evento.
- **Dados Pessoais (DP)**: Informação relacionada a pessoa natural identificada ou identificável.
- **Dado pessoal sensível**: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- **Controlador**: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
- **Operador**: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- **Cliente**: Uma organização que tenha um contato com um controlador de DP.
    - Um controlador de DP que tenha um contrato com um operador de DP.
    - Um operador de DP que tenha um contrato com um subcontratado para realizar tratamento de DP.
- **Encarregado pelo tratamento de dados pessoais**: Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- **Dado anonimizado**: Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- **Banco de dados para privacidade**: Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
- **Titular**: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- **Agentes de tratamento**: O controlador e o operador.
- **Tratamento**: Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
- **Anonimização**: Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
- **Consentimento**: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
- **Bloqueio**: Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

- **Eliminação**: Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.
- **Transferência internacional de dados**: Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.
- **Uso compartilhado de dados**: Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.
- **Autoridade nacional de proteção de dados – ANPD**: Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

3. Escopo

- **Liderança**: Os líderes de nossa organização são responsáveis por conhecer e aplicar as políticas de segurança definidas no nosso SGPI, garantindo o total envolvimento no propósito de atingir os objetivos de segurança da organização.
- **Envolvimento de pessoas**: É responsabilidade de todos os níveis de nossos colaboradores conhecer e atender a política do SGPI se envolvendo nas questões relacionadas à segurança, permitindo que as suas habilidades sejam usadas para a garantia e melhoria contínua do SGPI.
- **Processos e melhoria contínua**: É responsabilidade da alta direção, representante da direção e equipe de segurança estar constantemente alertas com relação aos procedimentos e processos estabelecidos no SGPI. Os mesmos devem ser regularmente revisitados e melhorados, garantindo a efetividade da política estabelecida no SGPI.
- **Relacionamentos externos**: É responsabilidade da nossa empresa garantir nossa política em questões internas e em relacionamentos externos quando nossos clientes, fornecedores e condomínio e outras partes interessadas não possuírem sua própria política da segurança da informação. Quando um cliente ou fornecedor nos apresentar uma política distinta da nossa, o representante da direção junto com a equipe da segurança da informação deve avaliar se a nova política afeta de alguma maneira nossa segurança e possui a liberdade de adotar neste relacionamento a política terceira.

4. Diretrizes

4.1. **Geral**

A informação é conhecimento ou dados que têm valor para o negócio da empresa. Esta informação pode ser armazenada em qualquer formato e para tanto deve ser adequadamente protegida. A informação está presente em diversas formas e independente da forma apresentada ou do meio pela qual é compartilhada ou armazenada deve ser utilizada unicamente para a finalidade para a qual foi autorizada.
A Política de Segurança da Informação tem como principal diretriz proteger a informação de diversos tipos de ameaças, acesso, destruição, divulgação ou modificação não autorizada, para garantir a continuidade dos negócios minimizando os danos e maximizando o retorno dos investimentos e a oportunidade de negócios.

4.2. **Ativos da Informação**

Os ativos associados à informação e aos recursos de processamento da informação estão identificados e inventariados.
Para cada ativo da informação está definido um proprietário que é responsável por assegurar que o mesmo seja utilizado conforme política de segurança da empresa.
As diretrizes para utilização adequada dos ativos são informadas durante o processo de contratação de pessoas. Ativos específicos possuem como responsável profissional capacitado para manipulação garantindo a devida utilização.

4.3. **Controle de Acesso**

Controle de acesso é um dos mecanismos utilizados para proteger fisicamente e logicamente o ambiente de TI. O acesso aos ativos de TI deve ser permitido somente a pessoas autorizadas de acordo com os itens desta Política de Segurança da Informação.
O direito de uso dos ativos é controlado e cedido no momento da contratação e cessado quando do término do vínculo com a empresa, momento em que os ativos físicos são recolhidos.
Caso o contratado tenha a necessidade de acesso ao um sistema corporativo específico, este será provido via autorização do gestor da informação envolvida.

4.4. **Controle de Acesso Físico**

Entrada de funcionários

O acesso a informação, equipamentos, documentos e áreas seguras são devidamente controlados para que somente pessoas autorizadas tenham acesso a estes recursos.
A identificação dos funcionários às instalações da empresa é controlado por dispositivo de segurança que garante acesso apenas ao pessoal autorizado.
Dentro das instalações os funcionários possuem acesso as áreas comuns, ambientes restritos são controlados por chave e o acesso é permitido via autorização do responsável.
Funcionários demitidos somente poderão entrar na empresa, devidamente acompanhados por um funcionário responsável.

Entrada de visitantes

Não existe restrição de horário para atendimento de visitante, porém é restrito o acesso de visitantes sem o devido acompanhamento de um funcionário responsável.
O visitante deverá passar pelos processos de segurança realizados pela portaria do condomínio e durante a visita nas instalações da iT.EAM será recebido e acompanhado por um responsável da empresa. Ao término da visita este será acompanhado até que deixe as instalações da empresa. Durante toda o prazo em que o visitante estiver nas instalações da iT.EAM, o mesmo deve estar no campo de visão de algum colaborador da empresa, exceção para lugares privados como sanitários.

Entrada de fornecedores

O acesso de fornecedores a iT.EAM deve ser realizado mediante solicitação de serviço ao fornecedor.
Um funcionário responsável deve acompanhar as atividades do fornecedor durante o período em que estiver nas instalações da empresa. Salvo atividade realizada fora do horário comercial sendo que devidamente formalizada e autorizada pelo funcionário responsável.
O prestador de serviço deve portar identificação capaz de certificar se trata da pessoa contratada para o serviço.

Mesa Limpa

Nossos funcionários devem adotar a prática de que nenhuma informação confidencial deve ser deixada à vista, seja ela em papel ou anotadas em lugar visível ou de possível acesso.
Especial atenção também deve ser dada quando da utilização de impressoras coletivas, recolhendo o documento impresso imediatamente.
Maiores informações política de mesa limpa e tela limpa.

Áreas de entrega e de carregamento

Possuímos pontos de acesso para entregas e carregamentos que são a portaria do edifício e a antessala de nossa instalação.
As encomendas devem ser recebidas e entregues nestes 2 pontos, exceto quando o volume o peso, ou outro fator inviabilizar a operação. Neste caso o pessoal deve ser identificado e acompanhado por um funcionário da iT.EAM durante todo o tempo em que estiver em nossas instalações.

4.5. **Controle de Acesso Lógico**

Acessos no processo de Contratação

Durante o processo de contratação nossos funcionários recebem a devida liberação de acesso lógico aos ativos da informação necessários as suas atividades.
O funcionário irá receber acesso aos ativos da informação, como rede e sistemas, e deverá se responsabilizar pelo sigilo das informações recebidas.
Não é permitido a nenhum funcionário fornecer sua senha de acesso a outros funcionários a não ser que solicitado pelo gestor com formalização do motivo pelo qual a senha está sendo solicitada e realizando a alteração da senha assim que a causa da solicitação seja tratada.
Acessos específicos não contemplados no processo de contratação deverão ser tratados diretamente com o responsável pelo ativo da informação.

Cancelamento de acessos

O processo de desligamento de funcionários realiza a retirada dos direitos de acesso aos diversos ativos de informação.

Acesso à internet

A iT.EAM disponibiliza acesso à internet a funcionários e visitantes, sendo que o acesso a visitantes é feita através de rede específica e apartada de nossa rede corporativa.
A internet disponibilizada pela iT.EAM aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que este uso não envolva conteúdo pornográfico, obsceno, fraudulento, difamatório, racialmente ofensivo, viole normas regulatórias como download de software não legalizado ou cause riscos a nossa infraestrutura.
É proibida a divulgação de informações confidenciais da organização em quaisquer grupos de discussão, listas ou bate-papos.
A falha em não seguir a política irá resultar em sanções que variarão desde procedimentos disciplinares, com avisos verbais ou escritos.

Acesso ao Correio Eletrônico

Todos os usuários de correio eletrônico estão habilitados a enviar e receber mensagens externas.
O padrão para criação de e-mail institucional é nome.sobrenome@it-eam.com. Em casos excepcionais, de duplicidade ou que causem constrangimento aos usuários, o padrão deverá ser revisto.
A conta de e-mail é disponibilizada exclusivamente para uso institucional, não sendo admitido para uso pessoal.

Acesso ao código-fonte

O acesso ao código-fonte de programa e de itens associados (como desenhos, especificações, planos de verificação e de validação) é restrito à área de desenvolvimento.
Todos os produtos gerados durante o ciclo de vida de desenvolvimento de sistemas devem estar armazenados em repositórios sujeitos a mecanismos de controle de acesso, garantindo que somente colaboradores autorizados tenham acesso.
Os códigos-fontes dos sistemas de informação de propriedade da iT.EAM devem ser adequadamente mantidos, incluindo o controle de versionamento, a correta classificação das informações e a proteção contra acessos ou alterações indevidas.

Retirada ou ajuste de acessos

A liberação de acessos a sistemas, diretórios, grupos de acessos ou perfis administrativos oferecidos aos usuários necessitam de revisão, para assegurar que os acessos estejam compatíveis com o cargo, a área de atuação e as funções exercidas. Devem ser submetidos a processo de revisão periódica:

- Acessos concedidos a sistemas e aplicações;
- Acessos concedidos a infraestrutura de TI.

A revisão de acesso a sistemas deverá ser feita conforme a classificação da informação contida em cada sistema, ou outro critério estabelecido pela Alta Direção.
O processo de revisão deverá ser executado a cada vez que o funcionário passar por uma mudança de cargo ou função ou em análise crítica a ser realizada anualmente pela equipe de segurança da informação.

Acesso privilegiado

As credenciais de acesso privilegiado, que correspondem ao acesso a atividades de administrador de sistemas ou ativos físicos, deverá ser concedida mediante aprovação do gestor com base na função e na necessidade para desenvolvimento das atividades do trabalho.

O compartilhamento do uso das credenciais de acesso privilegiado deve ser vedado. Contudo, caso haja necessidade de compartilhamento por questões técnicas, estas devem ser autorizadas pelo gestor com formalização do motivo pelo qual a senha está sendo solicitada e realizando a alteração da senha assim que a causa da solicitação seja tratada.
Todos os usuários detentores de ID de acesso privilegiado devem também possuir ID de acesso de atividades não privilegiadas, de forma que a utilização do acesso ocorra quando for estritamente necessário.

Uso de programas utilitários privilegiados

É proibido o uso de programas utilitários para acesso a informações relacionadas ao setor administrativo e financeiro.
O setor operacional utiliza política de gestão a vista, portanto é permitido o uso de programas utilitários pela equipe de consultoria para acesso as ferramentas do setor.

Acesso seguro aos sistemas e gerenciamento de senhas

O procedimento de logon deve divulgar apenas as informações necessárias as atividades de determinado funcionário, evitando fornecer a um usuário não autorizado informações indevidas.
As mensagens de ajuda do processo de logon não devem possuir dicas capazes de permitir um usuário não autorizado o acesso ao sistema.
Todo usuário deverá ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação.
O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal, e é responsável por qualquer ação executada com o seu login/senha
Não é permitido o compartilhamento, divulgação a terceiros ou anotações em papel da identificação pessoal.
Incentivamos o uso de senhas fortes, sugerimos que a senha possua ao menos à seguinte formação:

- 8(oito) ou mais caracteres;
- Inclusão de letras maiúsculas, minúsculas, números e caracteres especiais.

Não é permitido utilizar senhas fracas, como baseada em nomes próprios, dados pessoais tais como nome, data de nascimento, número de documentos entre outros.
Não é permitido aos nossos funcionários anotação de senha em lugar visível ou que possa ser acessado por outra pessoa.
As senhas dos sistemas da empresa devem ser alteradas sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha.
Incentivamos a não reutilização de senhas.
O funcionário, quando receber uma senha criada por terceiro, deve alterá-la em seu primeiro acesso para uma senha segura, conforme sugerido acima.

Acesso remoto

Disponibilizamos acesso remoto à nossa infraestrutura, desde que necessário à realização das atividades laborais da empresa através de conexão segura com aprovação do gestor da área e equipe de T.I.
As ferramentas que disponibilizamos acesso remoto, são testadas e atendem aos nossos requisitos de segurança.
O acesso à informação de nossos clientes é realizado através conexão segura e protegia por senha.
As informações da empresa que são armazenadas remotamente, devem ser feitas via software que garanta a segurança dos dados armazenados e o tráfego da informação.

Tela Limpa

Nossos funcionários, quando aplicável, devem bloquear todos os equipamentos, estações de trabalho e servidores em qualquer ausência temporária evitando o uso indevido do equipamento.
Maiores informações política de mesa limpa e tela limpa.

4.6. **Uso de Dispositivos Móveis**

Não permitimos acesso dos dispositivos móveis pessoais a nossa rede corporativa, de forma que todos os dispositivos móveis de nossos funcionários possuem permissão de acesso apenas a rede de convidados.
Os ativos móveis pessoais não são cadastrados como ativos da segurança da informação iT.EAM.
Os dispositivos móveis pessoais utilizados por nossos funcionários para atividades de trabalho devem ser protegidos por senha ou identificação visual.
Somente software licenciado pela iT.EAM pode ser utilizado em dispositivo móvel pessoal para atividades de trabalho.
Não é permitido que documento de trabalho seja armazenado em dispositivo móvel pessoal a não ser que dentro de repositório próprio de ferramenta licenciada pela iT.EAM.
Ativos móveis da empresa são cadastrados como ativos da segurança da informação e seguem todos os requisitos da política da informação da iT.EAM.
Não é permitido o armazenamento de DP em dispositivos móveis pessoais de nossos funcionários.
Quando for inevitável o armazenamento de DP em ativos móveis de nossa empresa, os mesmos devem ser identificados por etiqueta visível e o disco deve ser criptografado. Caso o dado pessoal venha de uma fonte não regular deve ser aberta uma SAC para tratamento junto ao comitê do SGPI.

4.7. **Segurança nas comunicações**

É proibido a utilização dos Sistemas de Informação com o fim de realizar ações que sejam contra a legislação e normas nacionais e internacionais que podem provocar danos intencionais na rede ou outros sistemas, prejudicando de forma intencional o tráfego da rede ou o acesso a recursos.

4.8. **Segurança com Fornecedores**

Acordos com terceiros, parceiros e fornecedores são estabelecidos e documentados garantindo que não existam desentendimentos entre as partes, com relação à obrigação de ambos com os requisitos de segurança aplicáveis.

4.9. **Segurança em visitas de Fornecedores**

No caso de visita a clientes em que normas de segurança são definidas para acesso a áreas seguras, é obrigatório que nossos funcionários participem de todos os treinamentos de segurança disponibilizados e sigam todas as orientações garantindo sua integridade física.

4.10. **Conformidades**

Através de nossa área Jurídica, identificamos e seguimos toda a legislação aplicável que regulamenta o negócio, bem como os aspectos de propriedade intelectual. Também garantimos apenas a utilização de softwares e licenças oficiais, homologadas e autorizadas para não infringir direitos de propriedade intelectual e direito autoral de fabricantes e seus representantes.

4.11. **Gestão de Incidentes de Segurança da Informação**

Uma instrução de trabalho foi estabelecida e descreve as diretrizes para a gestão de incidentes de Segurança da Informação, garantindo um enfoque consistente e efetivo de gerenciamento de incidentes, assegurando que fragilidades e eventos de segurança da informação sejam detectados, registrados, investigados e sempre que possível, prevenidos.
Todos os funcionários da empresa devem conhecer e seguir esta instrução.

4.12. **Gestão da Continuidade de Negócio**

Possuímos procedimento estabelecidos para a recuperação de serviços e processos críticos de forma a assegurar que suas atividades consideradas essenciais continuem a ser executadas e que os serviços críticos fiquem disponíveis para o usuário, em situação de crises ou indisponibilidades não programadas.

A Gestão da Continuidade de Negócio da iT.EAM conta com a adoção de ações mediante ocorrência de eventos externos decorrentes de caso fortuito ou força maior, bem como situações de calamidade pública declarados pelo Estado ou órgãos competentes que impliquem em risco para a continuidade da segurança ou do negócios da empresa e a integridade física de seus funcionários.

4.13. **Gestão de Melhoria Contínua**

A iT.EAM conta com vários recursos para Gestão de Melhoria contínua de seus processos e coloca à disposição das Partes Interessadas um recurso para contribuir com o aprimoramento de seus processos, SAC – Solicitação de Ação Corretiva.
As Partes Interessadas, caso identifiquem a necessidade ou possibilidade de qualquer ação corretiva ou preventiva em nossos processos, poderão contribuir enviando sugestões para sac@it-eam.com .
A Parte Interessada solicitante deverá informar no e-mail:

- Nome do solicitante
- Data da solicitação
- Necessidade de contatar autoridade competente e qual
- Se envolve dados pessoais ou não
- Descrição do Problema com Evidências (O que aconteceu? / O que poderia acontecer?)
- Causa Provável (Por que Aconteceu? / Por que poderia Acontecer?)
- Ação Proposta (O que fazer para não voltar a acontecer? / O que fazer para não acontecer?)
- Enviar evidências dos fatos narrados, se possível
- Informar se deseja receber resposta da ação proposta

As Solicitações de Ações Corretivas serão analisadas pelo Comitê de Privacidade da iT.EAM e caso aprovadas, as medidas serão adotadas, com publicação para Partes Interessadas e capacitação de seus Colaboradores e terceiros se aplicável.

5. Responsabilidades

5.1. **Usuários**

Conhecer e cumprir a Política de Segurança da Informação na íntegra;
Relatar ocorrências ou suspeitas de incidentes de segurança ao Comitê do SGPI.
Zelar pela segurança da informação.

5.2. **Gestor**

Ser agente multiplicador, informando, incentivando e conscientizando cada usuário a cumprir a Política de Segurança da Informação e Política de Privacidade da Informação;
Garantir que no momento da contratação, o prestador de serviço conheceu e aceitou a Política de Segurança da Informação e Política de Privacidade da Informação.

5.3. **Equipe do SGPI**

Ser guardião da informação e dados pessoais dentro da empresa;
Manter e melhorar o sistema da segurança da informação e proteção de dados pessoais;
Revisar e atualizar os documentos que compõem a Política de Segurança da Informação e Política de Privacidade da Informação;
Conscientizar e orientar os usuários em relação à Política de Segurança da Informação e Política de Privacidade da Informação;
Julgar os incidentes de segurança da informação e comunicar o resultado aos gestores para que as medidas disciplinares cabíveis sejam executadas;
Definir o conteúdo das informações que estarão disponíveis para os usuários.

5.4. **Área de Recursos Humanos**

Garantir, no momento da contratação, que o processo relacionado a segurança da informação e privacidade e proteção de dados pessoais seja executado.

6. Documentos relacionados

- Manual do SGPI;
- Política de Privacidade da Informação;
- Política de Controle de Acesso;
- Política de Segurança Física;
- Processo de Contratação de Pessoal;
- Política de Mesa Limpa e Tela Limpa;
- Política de Uso Aceitável dos Ativos.

7. Alterações da Política de Segurança da Informação

A presente Política de Segurança da Informação é revisada em intervalos regulares e pode ser alterada ou atualizada pela iT.EAM em razão de cumprimento de obrigações legais ou alterações relevantes nas atividades da empresa. Todas as alterações realizadas entram em vigor quando publicadas, a menos que indicado de outra forma.

DIRETRIZES PARA A UTILIZAÇÃO DOS RECURSOS DE TECNOLOGIA E INFORMAÇÃO

Publicado por: iT.eam em jul/2022

+55 (31) 4063-7340 | www.it-eam.com