

1. OBJETIVO

Gerar regras abrangentes, factíveis para as Áreas de Negócios em geral.

1.1. Missão

Garantir a disponibilidade, integridade, confidencialidade da informação necessária para a realização dos negócios da **PSM Company**.

1.2. Visão

Sermos reconhecidos como referência na prestação de serviços em tecnologia e gestão de Recursos Humanos

1.3. Valores

Acreditamos nas Pessoas e nelas investimos seguindo diretrizes como: Ética, Valorização da Diversidade, Transparência e Companheirismo.

2. APLICAÇÃO

Se aplica aos colaboradores interno, colaboradores externos e usuários.

3. REFERÊNCIAS

Não se aplica

4. DEFINIÇÕES

SI: Segurança da Informação – é a proteção da informação contra uma ampla gama de ameaças, s fim de garantir a continuidade dos negócios, minimizar riscos do negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio;

PSI: Política de Segurança da Informação e Privacidade ou Programa Segurança da Informação e Privacidade;

TI: Tecnologia da Informação;

Backup e Restore: é a cópia de dados de um dispositivo de armazenamento para que possa ser restaurado (restore) em caso de perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados;

Software: é a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. As interações dos colaboradores de computadores são realizadas através dele;

Mídias Removíveis: dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Pen Drive, cartão de memória e HD externo;

USB: é um tipo de conexão “ligar e usar” que permite a conexão de periféricos sem a necessidade de desligar o computador;

Firewall: é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

5. RESPONSABILIDADES

A responsabilidade pela proteção dos ativos corporativos de informação não é apenas da Área da Segurança da Informação, mas sim dos **colaboradores**. Cada um, colaborador ou usuário, tem de assegurar a confidencialidade, integridade e disponibilidade das informações, bem como pelo cumprimento da presente Política - Segurança da Informação e Privacidade.

Cabe aos **colaboradores** cumprir fielmente a Política - Segurança da Informação e Privacidade; buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação e privacidade; proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados; assegurar que os recursos tecnológicos à disposição sejam utilizados apenas para as finalidades aprovadas pela **PSM Company**; cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual; e comunicar imediatamente a Organização quando do descumprimento ou violação desta política.

6. PROCEDIMENTOS

O procedimento oriundo desta Política - Segurança da Informação e Privacidade é de responsabilidade dos Gestores das respectivas Áreas de Negócios envolvidas.

As políticas específicas por tema são tipicamente estruturadas para atender às necessidades de determinados grupos-alvo dentro da **PSM Company** ou para cobrir determinadas áreas de segurança.

A Política - Segurança da Informação e Privacidade é apoiada pelas seguintes políticas e normas, procedimentos e formulários específicos por tema:

- a. Controle de Acesso
- b. Segurança física e do ambiente;
- c. Gestão de Ativos;

- d. Transferência de informações;
- e. Configuração e manuseio seguros de dispositivos *endpoint* do usuário;
- f. Segurança de redes;
- g. Gestão de incidentes de segurança da informação;
- h. *Backup e Restore*
- i. Criptografia e gerenciamento de chaves;
- j. Classificação e tratamentos de informações;
- k. Gestão de vulnerabilidades técnicas;
- l. Desenvolvimento seguro;
- m. Aplicações Específicas
 - o Mesa Limpa e Tela Limpa
 - o Senhas
 - o Utilização de Dispositivos Pessoais – BYOD
 - o Utilização de Dispositivos móveis

6.1. Programa de Segurança da Informação e Privacidade

Sendo a Política - Segurança da Informação e Privacidade a base para o estabelecimento de os padrões de normas e procedimentos de segurança da informação e privacidade, sua abrangência é sobre os ambientes tecnológicos da **PSM Company** (como Redes Locais, Intranet, Internet).

Portanto, o compromisso dos colaboradores e usuários no cumprimento das diretrizes estabelecidas, é fundamental para a efetiva implementação da Política - Segurança da Informação e Privacidade na **PSM Company**.

Iniciativas relacionada à definição de normas ou procedimentos, bem como contratação de empresas, aquisição de produtos ou serviços inerentes à segurança da informação e privacidade, deverá ser submetida a Área de Segurança da Informação e Diretoria para apreciação e aderência à Política - Segurança da Informação e Privacidade.

6.2. Organização da Segurança

O objetivo da organização da Segurança da Informação e Privacidade é promover a gestão corporativa da área Segurança da Informação para a **PSM Company**, proporcionando uma proteção efetiva dos ativos de informação.

Na contratação do **colaborador** ou **usuário**, durante sua integração deve-se incluir tópicos referentes à segurança da informação e privacidade, ou mesmo referir-se aos documentos oficiais da **PSM Company** sobre o tema. O contrato, deve, necessariamente, estabelecer que o documento Política - Segurança da Informação e Privacidade, Política de Privacidade de Dados, Código de Ética e Código de Conduta sejam cumpridos na íntegra e, ainda, fixar as penalidades decorrentes de violação das regras de segurança da informação e privacidade definidas.

A Política - Segurança da Informação e Privacidade define as responsabilidades e competências relacionadas às áreas supracitadas.

6.2.1. Violações

São consideradas violações à Política - Segurança da Informação e Privacidade as seguintes situações, não se limitando às mesmas:

- a)** Quaisquer ações ou situações que possam expor a **PSM Company** à perda financeira ou de imagem, ou de marca, ou de reputação, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;
- b)** Uso indevido de dados corporativos, divulgação não autorizada de informações, segredos comerciais sem a permissão expressa do Gestor da Informação;
- c)** Uso de dados, informações, equipamentos, software, sistemas ou recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, código de ética, código de conduta ou de exigências de organismos reguladores da área de atuação da **PSM Company**;
- d)** A não comunicação imediata de quaisquer descumprimentos da Política - Segurança da Informação e Privacidade, que porventura um **colaborador ou usuário** venha a tomar conhecimento ou chegue a presenciar;
- e)** Efetuar declarações verbais, escritas em meios de comunicação seja ela mídia digital ou verbal em nome da **PSM Company** ou ainda mencionando a mesma sem que tenha autorização formal para esse fim.

6.2.2. Sanções

A violação a um controle de segurança ou a não aderência à Política - Segurança da Informação e Privacidade e suas definições são consideradas faltas graves ou violações, podendo ser aplicadas penalidades ou sanções de acordo com a deliberação, como segue:

- a) Aplicação de sanções trabalhistas previstas em legislação vigente, incluindo dispensa por justa causa;
- b) Abertura de Processo civil ou criminal;
- c) Término ou cessão do contrato de prestação de serviço ou relação comercial;
- d) Imediato ressarcimento dos prejuízos causados à **PSM Company**;
- e) Aplicação de ações punitivas constantes na legislação brasileira vigente ou nos códigos de ética, código de conduta e relacionamento, civis e comerciais;
- f) Quando a infração se der em outros países se aplicam as punições relativas ao mesmo além das punições constantes do **item e**;

Classificação de Nível de Incidente – Contexto Trabalhista

Tipo	Sanção
Grave	Advertência
Muito Grave	Suspensão
Gravíssimo	Desligamento

Reincidência:

No caso de reincidência nos incidentes considerados Grave passa a ser Muito Grave;

No caso de reincidência Muito Grave passa a ser, Gravíssimo.

6.3. Regras Gerais

As regras abaixo discriminadas aplicam-se as áreas da **PSM Company** assim distribuídas:

- a) Atuar em conjunto com a Área de Tecnologia da Informação na elaboração ou desenvolvimento de dispositivos de Segurança da Informação e Privacidade, específicos, se necessário;

- b) Reavaliar, periodicamente, as autorizações dos **colaboradores** que acessam os ativos de informação sob sua responsabilidade, cancelando os que não tenham mais necessidade de acessar os ativos de informação;
- c) Promover e garantir o treinamento adequado aos **colaboradores** sob sua responsabilidade;
- d) Envolver a Área de Tecnologia da Informação nos incidentes de segurança;
- e) Informar o incidente de segurança a Área de Segurança da Informação e Privacidade;
- f) Realizar ações de conscientização em segurança da informação e privacidade sob demanda, para a **PSM Company**, ações estas delegadas pela Área de Segurança da Informação;
- g) A **PSM Company** disponibiliza um único e exclusivo e-mail, para cada um de seus colaboradores e este, e somente este, deve ser utilizado pra trocas de informação entre os colaboradores;
- h) Informar, quando cabível, a Área de Segurança da Informação os resultados das revisões independentes e dos testes de acesso, de forma que possam ser elaboradas as alterações necessárias no Programa de Segurança da Informação e Privacidade e os planos de ação necessários para a correção dos desvios;
- i) Solicitar aos Colaboradores da base administrativa da **PSM Company** que **NÃO consumam, sob nenhuma hipótese, alimentos e/ou líquidos nas suas estações de trabalho, pois isto se configura uma violação grave.**
Exceção: A única exceção a isso é a utilização de Garrafa / Squeeze apropriada para acondicionamento de água potável, possibilitando assim o consumo dela na estação de trabalho;
- j) Solicitar aos Colaboradores da base administrativa da **PSM Company** que **desliguem** seus equipamentos que ficam ligados sem o uso imediato (filtros de linha, carregadores de celular) ou ao término da jornada de trabalho. Equipamentos ligados por tempo indeterminado podem causar princípios de incêndios;
- k) Assegurar que os Colaboradores da base administrativa da **PSM Company** usem de forma tempestiva o crachá em local visível;