POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

A Pólvora estabelece que todos os colaboradores, prestadores de serviços, parceiros e quaisquer terceiros que tenham acesso às suas informações e recursos tecnológicos devem observar e cumprir integralmente as diretrizes previstas na Política de Segurança da Informação – FR-SEG002, ou outra que venha a substitui-la.

É obrigatória a manutenção do mais absoluto sigilo sobre todas as informações acessadas em razão da relação com a Pólvora, sendo vedada sua divulgação, reprodução ou utilização para quaisquer finalidades sem prévia e expressa autorização da Diretoria.

Os recursos tecnológicos disponibilizados destinam-se exclusivamente a fins profissionais, sendo proibida sua utilização para armazenamento ou processamento de arquivos pessoais, bem como o depósito destes em estações de trabalho ou servidores corporativos.

A Pólvora poderá, a qualquer tempo e conforme necessário, realizar acessos remotos, auditorias e monitoramentos nos sistemas, equipamentos, e-mails corporativos, navegação na internet e arquivos, com o objetivo de garantir a integridade, a confidencialidade e a segurança das informações, em conformidade com a legislação aplicável e as normas internas.

O uso inadequado dos recursos tecnológicos, bem como o descumprimento das diretrizes de segurança da informação, poderá ensejar a adoção das medidas cabíveis, de natureza administrativa, contratual, trabalhista, civil e/ou penal, conforme o caso, tudo conforme detalhamento a seguir

Introdução:

A Tecnologia da Informação, TI, está cada dia mais presente nas empresas, mudando radicalmente os hábitos e a maneira de comunicação, sendo de vital importância a definição de normas de segurança que visem disciplinar o uso da tecnologia da informação.

A **Pólvora** baseada na norma **NBR ISO/IEC 27.002** e demais aplicáveis à espécie definiu sua Política de Segurança da Informação – PSI, conscientizando e definindo as normas e procedimentos necessários para proteger a confidencialidade das informações e a continuidade dos negócios.

Objetivo:

Definir responsabilidades e orientar a conduta dos usuários da Pólvora, visando a continuidade dos negócios através da confidencialidade, da integridade e da disponibilidade das informações da **Pólvora.**

Aplicação:

Esta PSI aplica-se a todos os usuários da Pólvora e a qualquer colaborador ou pessoa custodiante de informações da Pólvora ou de seus clientes.

Princípios:

A informação produzida ou recebida como resultado de sua atividade profissional pertence à **Pólvora**.

Divulgar informações confidenciais ou estratégicas é crime previsto nas leis de propriedade intelectual, industrial (Lei nº 9279) e de direitos autorais, (Lei nº 9610).

A segurança da informação depende de pessoas comprometidas, processos gerenciais de controle e sistemas de segurança da informação.

Usuários de Informática:

São reconhecidos como usuários da infraestrutura de TI todos os colaboradores, profissionais autônomos, temporários ou de empresas prestadoras de serviço que obtiverem a aprovação por escrito do responsável hierárquico e da gestão de liberações da **Pólvora**, para prescrição de senhas de acesso aos recursos computacionais.

Responsabilidades:

A **Pólvora** entende que o sistema de segurança da informação somente será eficaz com o comprometimento de TODOS!

Dos Usuários

- Respeitar esta Política de Segurança da Informação
- Responder pela guarda e proteção dos recursos computacionais colocados á sua disposição para o trabalho;
- Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
- Ativar suas senhas de proteção para Correio Eletrônico e Sistema Operacional, sob orientação;
- Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software.
- Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc;

- ☐ Assegurar que as informações e dados de propriedade da **Pólvora** não sejam disponibilizados a terceiros, a não ser com autorização por escrito do responsável hierárquico.
- Comprometer-se em não auxiliar terceiro ou não provocar invasão dos computadores ou da rede de dados, conforme artigo 154-A do Código Penal Brasileiro.
- Relatar para o seu responsável hierárquico e à Gerência de TI, o surgimento da necessidade de um novo software para suas atividades.
- ☐ Responder pelo prejuízo ou dano que vier a provocar a **Pólvora** ou a terceiros, em decorrência da não obediência as diretrizes e normas aqui referidas.

Dos Responsáveis Hierárquicos:

- Apoiar e zelar pelo cumprimento desta PSI, servindo como modelo de conduta para os colaboradores sob a sua gestão.
- Atribuir na fase de contratação e de formalização dos contratos individuais de trabalho CLT, prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI.
- Autorizar o acesso e definir o perfil do usuário,
- Autorizar as mudanças no perfil do usuário,
- Educar os usuários sobre os princípios e procedimentos de Segurança da Informação,
- Notificar imediatamente a Pólvora quaisquer vulnerabilidades e ameaças a quebra de segurança;
- Assegurar treinamento para o uso correto dos recursos computacionais e sistemas de informação;
- Advertir formalmente o usuário e aplicar sanções cabíveis quando este violar os princípios ou procedimentos de segurança, relatando imediatamente o fato.
- Obter aprovação técnica antes de solicitar a compra de hardware, software ou serviços de informática.
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

Da Área de TI

- Configurar os equipamentos e sistemas para cumprir os requerimentos desta PSI,
- Testar a eficácia dos controles utilizados e informar os riscos residuais.
- Restringir a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Garantir segurança do acesso publico e manter evidências que permitam a rastreabilidade para auditoria ou investigação.
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.
- ☐ Administrar, proteger e testar as cópias de segurança dos programas e dados ao negócio da **Pólvora**.
- Gerenciar o descarte de informações a pedido dos custodiantes.
- Garantir que as informações de um usuário sejam removidas antes do descarte ou mudança de usuário.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
- Criar a identidade lógica dos colaboradores na Pólvora.
- Atribuir contas e senhas identificáveis a pessoa física para uso de computadores, sistemas, bases de dados e qualquer outro ativo de informação.
- Proteger todos os ativos de informação da Pólvora contra códigos maliciosos e ou vírus.
- Garantir que processos de mudança não permitam vulnerabilidades ou fragilidades no ambiente de produção.
- Definir as regras formais para instalação de software e hardware, exigindo o seu cumprimento dentro da Pólvora.
- Realizar inspeções periódicas de configurações técnicas e análise de riscos.

- Gerenciar o uso, manuseio e guarda de assinaturas e certificados digitais.
- Garantir assim que solicitado o bloqueio de acesso de usuários por motivo de desligamento da Pólvora,
- Propor as metodologias sistemas e processos específicos que visem aumentar a segurança da informação,
- Promover a conscientização dos colaboradores em relação a relevância da segurança da informação,
- Apoiar a avaliação e a adequação de controles de segurança da informação para novos sistemas ou serviços.
- Buscar alinhamento com as diretrizes corporativas da Pólvora.
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.
- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas pode ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- ☐ Monitorar o ambiente de TI a capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso a internet e aos sistemas críticos da **Pólvora**, indisponibilidade aos sistemas críticos, incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); atividade de todos os colaboradores durante os acessos as redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior), conforme procedimento publicado na matriz de responsabilidade.
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

Identificação - Login e Senha:

- Os sistemas de Login e senha protegem a identidade do usuário, evitando e prevenindo que uma pessoa se faça passar por outra. Código Penal Brasileiro art. 307 – falsa identidade.
- Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade será dos usuários que dele se utilizarem.
- Os usuários deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %).
- É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.
- As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), não devem ser baseadas em informações pessoais, como próprio nome, familiares, nascimento, endereço, placa de veículo, nome da empresa, e ou não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.
- Os usuários devem proceder a troca de senha, caso suspeitem de quebra por terceiros ou obrigatoriamente a cada 4 meses ou terão seus acessos bloqueados automaticamente.
- O Login e Senha devem ser imediatamente bloqueados quando se tornarem desnecessários.
- Tentativa de violação e burla de senhas de acesso, criptografia ou identificação biométrica se identificada será alvo de ação disciplinar.
- ☐ Os acessos externos à rede de informações da **Pólvora** fora do expediente de trabalho serão bloqueados atendendo a Lei 12.551, tele trabalho que altera o Art. 6º da CLT, exceto para cargos de confiança.

Recursos Computacionais:

- ☐ Os recursos de TI alocados pela **Pólvora** aos seus usuários são destinados exclusivamente às atividades relacionadas ao trabalho, sendo proibido o uso dos mesmos com para fins pessoais.
- ☐ Aos colaboradores da **Pólvora** fica proibido o uso de equipamentos de tecnologia, como computadores, tablets, notebooks, netbooks e similares de propriedade particular nas dependências da Pólvora.

- É proibida a intervenção do usuário para manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, bem como a transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros (pirataria).
- Todo computador em desuso, deverá ser encaminhado à área de TI para a remoção das informações, descarte ou reuso.

Tela Limpa e Mesa Limpa

- ☐ O papel de parede e proteção de tela de todos os micros deverá seguir a padronização da **Pólvora**.
- O usuário deve cuidar para que papéis, mídias e imagens nos monitores não fiquem expostas ao acesso não autorizado.
- Os computadores deverão ser bloqueados por senha quando não estiverem sendo utilizados.

Descarte de Mídias

- ☐ Mídias contendo informações referentes a **Pólvora,** deverão ser destruídas antes de seu descarte.
- CD's, DVD's, e documentos em papel deverão passar pelo triturador antes de serem encaminhadas ao lixo, HD's deverão ser encaminhados a TI para a destruição da informação antes do descarte ou reutilização.

Antivírus:

- ☐ O escritório **Pólvora,** por intermédio da área de TI, disponibiliza software corporativo de antivírus instalado para todos os usuários.
- O antivírus é atualizado automaticamente na estação de trabalho do usuário sempre que uma nova versão é disponibilizada pelo fabricante através do aplicativo servidor;
- ☐ A área de TI da **Pólvora** não recomenda que o usuário remova ou altere as configurações do antivírus a fim de não comprometer a segurança que o fabricante do software proporciona.
- As checagens periódicas do disco rígido, HD, da estação de trabalho esta programada para execução periódica automática conforme definições da área de TI no aplicativo servidor.

Armazenamento de Arquivos:

- ☐ Todos os arquivos contidos nos servidores de rede ou nas estações de trabalho dos usuários devem ser exclusivamente de interesse da **Pólvora**.
- É proibida a criação de pastas pessoais nos servidores de rede.
- ☐ A criação de pastas departamentais nos servidores de rede deverá refletir a estrutura organizacional da **Pólvora a** e ser solicitada pelo responsável hierárquico.
- O acesso às pastas departamentais nos servidores de rede exige autorização do responsável para o controle do acesso de cada usuário.
- ☐ Todos os arquivos que não sejam do interesse da **Pólvora** deverão ser excluídos dos equipamentos para evitar problemas futuros com as auditorias.

Salvaguarda de Arquivos:

- Compete à área TI criar e manter cópias de segurança (backups) apenas dos dados armazenados nos servidores de rede;
- ☐ Os usuários devem manter obrigatoriamente os documentos, planilhas, e-mails, apresentações, desenhos, e outros dados críticos da **Pólvora**, nas pastas departamentais dos servidores de rede;
- É de responsabilidade exclusiva do usuário a cópia de segurança (backup) e a guarda dos dados gravados da sua estação local de trabalho.

Utilização da Internet:

- A Internet foi instalada para viabilizar a busca de informações e agilizar determinados processos da **Pólvora**, sendo proibido o uso pessoal da ferramenta.
- O uso indevido do acesso à Internet é de inteira responsabilidade do usuário, podendo o mesmo ser responsabilizado legalmente pelos danos causados.
- A auditoria dos acessos à Internet leva ao conhecimento dos responsáveis hierárquicos, relatórios com nomes dos usuários, páginas consultadas, tempo de consulta, e o conteúdo navegado.

Jogos:

- Jogos estão terminantemente proibidos.

Softwares Piratas:

- Os softwares homologados e instalados nos computadores e servidores de rede são de propriedade exclusiva da **Pólvora**, sendo proibidas as cópias integrais, ou mesmo as parciais, bem como a instalação de softwares piratas.
- Pirataria é considerada crime e softwares piratas causam prejuízos tanto materiais como funcionais além de denegrir a imagem da Instituição. Por esta razão, estão terminantemente proibidos.
- A instalação de softwares não autorizados (Pirataria) constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, e o infrator está sujeito à pena de detenção e multa;

Email e Mensagens instantâneas

- É proibido o uso de e-mails, correios eletrônicos ou mensagens instantâneas de forma contrária a lei, a moral, aos bons costumes, à ordem pública ou que infrinjam os direitos a propriedade intelectual ou industrial pertencente a terceiros.
- O conteúdo e a utilização de e-mails, correios eletrônicos ou mensagens instantâneas deve ser de caráter exclusivamente profissional.
- Os serviços de mensagens instantâneas são permitidos apenas para os usuários autorizados pela hierarquia da **Pólvora**.
- A salvaguarda do conteúdo anexo é de responsabilidade exclusiva do usuário, ficando **Pólvora** isento de tal obrigação.
- É proibido o uso de software de e-mail, mensagens instantâneas e correio interno **não homologados** são de responsabilidade do usuário e podem trazer riscos a segurança da informação além de dificultar o suporte técnico.
- Mensagens recebidas de origem desconhecida deverão ser previamente visualizadas e eliminadas imediatamente, sem leitura de seu conteúdo, para evitar contaminação por vírus e outros riscos.
- O uso indevido do e-mail é de inteira responsabilidade do usuário, podendo o mesmo ser responsabilizado pelos danos causados.
- As mensagens trafegadas sob o domínio da **Pólvora** poderão ser auditadas, mediante solicitação, conforme definição do TST, Tribunal Superior do Trabalho. Desta forma é proibida a utilização particular.
- Em nenhuma hipótese o **Pólvora** será responsabilizado perante quaisquer usuários ou terceiros pela perda de mensagens e/ou respectivo conteúdo.
- O fato do colaborador responder a um e-mail fora do horário de expediente não configurará hora extra. Para que isto ocorra é necessário que o **Pólvora** tenha exigido na demanda enviada por e-mail, a realização de uma tarefa fora do horário de trabalho.

Auditorias e acesso remoto

- Auditorias serão realizadas e relatórios serão gerados periodicamente ou conforme solicitações de acordo com os procedimentos da área de TI.

- O acesso remoto, ou auditoria de dados locais, quando realizados no equipamento de uso do colaborador não caracteriza invasão do mesmo, pois o equipamento é de propriedade da Pólvora, e todas as informações contidas no mesmo são de propriedade da **Pólvora**, uma vez que o usuário é proibido de salvar dados pessoais nos equipamentos de tecnologia da **Pólvora**.
- Poderão ser solicitados relatórios de auditoria contendo o nome, mensagens trafegadas, acessos a Internet e demais informações do usuário conforme resolução do TST.

Disposições Finais

- Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da **Pólvora**. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

Todas as práticas que ameacem à segurança da informação serão tratadas com a aplicação de ações disciplinares, desde uma advertência verbal até rescisão contratual por justa causa, levando em consideração fatores como: função exercida pelo colaborador, período utilizado, local de utilização, horário de utilização, prejuízo real ou potencial causado a **Pólvora**, entre outros