PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Esta política tem como principal objetivo, documentar e proteger todo e qualquer tipo de informação trafegado dentro das unidades do Grupo São Roque consideradas importantes para continuidade dos objetivos de negócio da organização, padronizando e estabelecendo os requisitos mínimos de segurança de rede, dispositivos, processos e pessoas.

Para que isso seja possível, os serviços realizados pela Symerp Tecnologia de consultoria em gestão e planejamento de t.i utiliza ferramentas de controle e monitoramento de processos seguindo a boas práticas da biblioteca ITIL (Technology infrastructure Library) que tem como objetivo concentrar-se no alinhamento de serviços de TI com as necessidades de negócio, alcançamos esse objetivo com ajuda de um software web chamado MILVUS, com ele controlamos acessos, realizamos monitoramento e acompanhamento de SLA, técnicos e colaboradores através de um aplicativo instalado em todos os dispositivos (computadores) e ativos de rede (infra) onde garantimos de forma preventiva o funcionamento de todo o parque de tecnologia, garantindo assim a proteção das informações entre os clientes e a empresa nos aspectos de confidencialidade, integridade e disponibilidade.

- **Confidencialidade** – Garantia de que o acesso à informação seja obtido, apenas, por pessoas autorizadas. A quebra desse sigilo pode acarretar danos inestimáveis para a empresa ou até mesmo para uma pessoa física (cliente), portando o controle a informação é gerido de acordo com o organograma da hierarquia e auditoria de acesso, estes formulados pelos líderes de setores, estes que podem solicitar ao departamento de tecnologia informações de quem, quando como alterou, moveu ou excluiu determinado dado.

- **Integridade** – Garantia de que a informação não seja adulterada falsificada ou furtada. Para que isso ocorra de forma automatizado foi implantado política de grupo, setores e acessos com auditoria de arquivos alterados e por quem. Copias sombras dos dados são realizadas através de versões anteriores para comparativos de informação via hash.

- **Disponibilidade** – Garantia de que a informação esteja disponível sempre que requisitada pelos usuários autorizados mesmo com as interrupções involuntárias de sistemas, ou seja, não intencionais.

A PSI aplica-se a todos os usuários da empresa e a qualquer colaborador ou pessoa custodiante de informações do Grupo São Roque e Symerp Tecnologia ou de seus clientes.

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

Segurança e Backup contra perca de dados

Todo o Banco de dados e aplicação do sistema Shift Lis (Sistema de gestão ERP) do grupo São Roque ficam 100% em nuvem alocados nos Datacenters da Equinix que possuem um alto nível de disponibilidade e redundância contra perda de dados ou informações.

O grupo São Roque possui 4 servidores locais divididos por região, esses servidores possuem banco de dados local com o sistema Shift Automação, responsável pela coleta dos resultados lidos nos equipamentos médicos. O backup desse banco de dados é realizado a cada 4 horas localmente em disco externo e migrado para nuvem da Symerp Cloud, empresa do grupo Symerp a cada 12 horas, que por sua vez realiza cópias para os Datacenters da GreenHouse (NL), OVH Hosting(CA) e TeleHouse(DE) como forma de redundância via aplicação Nextcloud com proteção anti Ransonware.

Arquivos e documentos localizados nos computadores de cada colaborador recebem um sistema de backup via IPERIUS onde é feito um backup automático na nuvem da Symerp Cloud uma vez ao dia. Os líderes de setores possuem usuários exclusivos e mapeados para acesso as informações contidas na nuvem com acesso de qualquer local. Demais colaboradores possuem acesso somente leitura apenas de dentro da sede do Grupo São Roque.

O Grupo Symerp entende que o sistema de segurança da informação somente será eficaz com o comprometimento de TODOS!

LGPD

Este Termo tem como objetivo reforçar o compromisso do Grupo São Roque com a privacidade e com o cumprimento da Lei Geral de Proteção de Dados, lei 13.709/2018 - LGPD, que protege os direitos dos titulares dos dados de forma clara e objetiva.

Até a presente data foi implantado pela Symerp Tecnologia no site institucional do Grupo São Roque o termo de consentimento de cookies e apresentação do documento sobre a política de privacidade praticado. O mesmo possui monitoramento em tempo real que dá ao titular dos dados obtidos (cliente) pelo grupo São Roque o direto de saber e realizar solicitações tais como, atualização de dados cadastrados, confirmação de existência de dados no banco de dados do grupo, fazer solicitação de exclusão permanente dos dados, solicitar portabilidade dos dados, solicitar acesso aos dados cadastrais. O sistema implantado faz o filtro

das requisições do titular e faz o encaminhamento para o DPO (Encarregado de dados) tomar as ações cabíveis junto ao titular, ANPD e o Grupo São Roque.
OBS: O cargo de DPO ainda não foi atribuído a nenhum colaborador ou empresa especializada, estamos em fase de adequação.

Comprometimento dos Usuários

- Respeitar esta Política de Segurança da Informação
- Responder pela guarda e proteção dos recursos computacionais colocados à 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 do Gestor de Liberações da área de TI;
- 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 do Grupo São Roque 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 ao Grupo São Roque ou a terceiros, em decorrência da não obediência as diretrizes e normas aqui referidas.

Comprometimento 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 junto ao gestor de liberações da área de TI,
- Autorizar as mudanças no perfil do usuário junto ao gestor de liberações da área de TI,
- Educar os usuários sobre os princípios e procedimentos de Segurança da Informação,
- Notificar imediatamente ao gestor de liberações da área de TI 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 ao gestor de liberações da área de TI.
- Obter aprovação técnica do gestor de liberações da área de TI 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.

Comprometimento da Área de Gestão de TI

- Configurar os equipamentos e sistemas para cumprir os requerimentos desta PSI,
- Testar a eficácia dos controles utilizados e informar aos gestores 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 público 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.
- Gerenciar o descarte de informações a pedido dos solicitantes.
- 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 garantindo a segurança por área do negócio.
- Criar a identidade lógica dos colaboradores na empresa.
- 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 empresa 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 empresa.
- 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 empresa,
- 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 empresa.
- 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 através da capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso à internet e aos sistemas críticos do Grupo São Roque, 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;

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

Bebedouro, 07 de outubro de 2021.

Gestão de Tecnologia da Informação