POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI.
SGS POLÍMEROS.

TIPO DE DOCUMENTO:	CLASSIFICAÇÃO:	VERSÃO:
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO INTEGRANTE DO SGSI - SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO.	INTERNO	002
IDENTIFICADOR ÚNICO: P_SEGURANÇA_DA_INFORMAÇÃO_SGS_03_2024.	**DATA:** 19/03/2024	**PÁGINA:** 1/32

CONTROLE DE APROVAÇÃO:

AUTOR:	CARGO:	DATA:
LUIS CARLOS MOUTINHO GARCIA	DPO	19/03/2024
REVISÃO LUIS CARLOS MOUTINHO GARCIA	CARGO: CONTROLLER	DATA: 19/03/2024
APROVAÇÃO: NEI EDUARDO SCHNEIDER	CARGO: DIRETOR	DATA: 19/03/2024

CONTROLE DE VERSÕES/ MODIFICAÇÕES

VERSÃO:	DATA:	ALTERAÇÕES EM RELAÇÃO À EMISSÃO ANTERIOR
VERSÃO: 001	DATA: 01/09/2021	ALTERAÇÕES EM RELAÇÃO À EMISSÃO ANTERIOR EMISSÃO INICIAL
VERSÃO: 002	DATA: 19/03/2024	ALTERAÇÕES EM RELAÇÃO À EMISSÃO ANTERIOR **SUBSTITUIÇÃO DPO**
VERSÃO: 003	DATA:	ALTERAÇÕES EM RELAÇÃO À EMISSÃO ANTERIOR

SUMÁRIO

1. OBJETIVO:

Determinar e informar as Diretrizes e Normas Administrativas em Tecnologia da Informação da empresa SGS POLÍMEROS através das seguintes regras:

I. Estabelecer diretrizes que permitam aos colaboradores e prestadores de serviços da SGS POLÍMEROS, seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo, norteando a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

II. Preservar as informações da SGS POLÍMEROS quanto à:

Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

III. **Sobre a Lei 13.709/2018 (LGPD)** – Esta política possui a relevância sobre a forma de tratamento das informações (dados identificáveis e (ou) sensíveis) dos colaboradores, e (ou) Prestadores de serviços que tratam dados identificáveis estritamente necessários e justificados em nome do controlador (SGS POLÍMEROS), Informações de tratamento devidamente ratificadas através das declarações (anexas) aos contratos de prestação de serviços e (ou) acordo de trabalho entre o Controlador e Operadores de dados subordinados. Estes documentos, permanecem em constante atualização e identificados por indicadores únicos e de versões aprovadas. Esta declaração, torna-se respaldada pelas seguintes bases legais da LGPD: (**Consentimento, Legítimo interesse, Contratos, Obrigação legal, Execução de políticas públicas, Estudos de órgãos de pesquisa, Processo Judicial, Proteção à vida, Tutela da vida, Proteção ao crédito**), e obedece os seguintes princípios para o tratamento destas informações: (**Finalidade, Adequação, Livre Acesso,**

Necessidade, Qualidade dos dados, Transparência, Segurança, Prevenção, Não discriminação, Prestação de contas).

2. ABRANGÊNCIA:

Colaboradores internos e prestadores de serviços da SGS POLÍMEROS.

I. As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, inclusive prestadores de serviço; e se aplicam à informação em qualquer meio ou suporte. Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

II. É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Sistemas sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

3. DEFINIÇÕES:

PSI: Política de Segurança da Informação.
DPO: Data Protection Officer – Encarregado de Proteção de Dados.

4. CONTROLE:

O controle é efetuado pelo Encarregado de proteção de dados (DPO), pelo Comitê de Privacidade e Segurança da Informação da organização e de acordo com a legislação vigente, especificamente, com a Lei 13.709/2018 (LGPD) – Lei Geral de Proteção de Dados e o padrão IMS2 PECB ISO/27001 – SGSI.

5. APLICABILIDADE DESTA POLÍTICA:

I. Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela SGS POLÍMEROS pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

II. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

III. A SGS POLÍMEROS, por meio da Gerência de Sistemas, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

6. INTEGRAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

I. Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da SGS POLÍMEROS a fim de que a política seja cumprida dentro e fora da empresa.

II. Deverá haver um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designado como Comitê de Privacidade e Segurança da Informação.

III. Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança.

IV. Deverá constar em todos os contratos da SGS POLÍMEROS o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

V. A responsabilidade em relação à segurança da informação deve ser comunicada em quaisquer fases de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar esta Política de Segurança da informação.

VI. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Gerência de Sistemas e ela, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Privacidade e Segurança da Informação para análise.

VII. Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

VIII. Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

IX. Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pela SGS POLÍMEROS ou por terceiros.

X. Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

XI. A SGS POLÍMEROS exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis para garantir as bases legais previstas na Lei 13.709/2018 – Lei Geral de Proteção de dados, mantendo atualizado, um SGSI, Sistema de Gestão de Segurança da Informação norteado pelas cláusulas de 4 a 10 da norma ISO/IEC 27001:2013 e da Extensão de privacidade ISO/IEC 27001:2019.

XII. Esta PSI será implementada na SGS POLÍMEROS por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou de prestação de serviço.

XIII. O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação representará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

DAS RESPONSABILIDADES ESPECÍFICAS:

IX. Dos Colaboradores em Geral. - Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição, mas a ela vinculada.

X. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a SGS POLÍMEROS e/ou a terceiros, em decorrência da sua não observância às diretrizes e normas aqui referidas.

DOS COLABORADORES EM REGIME DE EXCEÇAO TEMPORÁRIOS:

XI. Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Privacidade e Segurança da Informação desta política.

XII. A concessão de acesso a informações poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

DOS GESTORES DE PESSOAS E (OU) PROCESSOS:

XIII. Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

XIV. Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI, bem como normas, instruções, códigos de postura, acordos de confidencialidade internos da SGS POLÍMEROS.

XV. Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da SGS POLÍMEROS;

XVI. Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

XVII. Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender aos termos desta PSI.

DOS CUSTODIANTES DA INFORMAÇÃO – ÁREA DE TECNOLOGIA

XVIII. Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;
Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes;

XIX. Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI e pelas Normas de Segurança da Informação complementares;

XX. Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente;

XXI. Segregar as funções administrativas, operacionais e técnicas a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações;

XXII. Garantir segurança essencial para sistemas com acesso público, incluindo o ambiente operacional, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;

XXIII. Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências;

XXIV. Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a SGS POLÍMEROS;

XXV. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela;

XXVI. O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante;

XXVII. Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário;

XXVIII. Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;

XXIX. Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

(a) Os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário;

(b) Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

XVIII. Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado;

XIX. Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros;

XX. Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa;

XXI. Realizar auditorias periódicas de configurações técnicas e análise de riscos;

XXII. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais;

XXIII. Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa;

XXIV. Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro;

XXV. Monitorar o ambiente de TI, gerando indicadores e históricos de:

(a) Ameaças detectadas e mitigadas;

(b) Restauração de serviços essenciais PCN;

(c) Detecção e controle de spams e phinshing scans;

(d) Índice de detecção e resposta à incidentes;

(e) Atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet, quando sob a utilização de dispositivos corporativos (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

XVIII. Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação;

XIX. Propor e apoiar iniciativas que visem à segurança dos ativos de informação SGS POLÍMEROS publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Comitê de Privacidade e Segurança da Informação;

XX. Promover a conscientização dos colaboradores em relação à relevância da privacidade (LGPD) e segurança da informação para o negócio da SGS POLÍMEROS, mediante campanhas, palestras, treinamentos e outros meios de endomarketing;

XXI. Apoiar a avaliação e a adequação de controles específicos de privacidade e segurança da informação para novos sistemas ou serviços;

XXII. Analisar criticamente incidentes em conjunto com o Comitê de Privacidade e Segurança da Informação;

XXIII. Apresentar as atas e os resumos das reuniões do Comitê de Privacidade e Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria;

XXIV. Manter comunicação efetiva com o Comitê de Privacidade e Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar SGS POLÍMEROS;

XXV. Buscar alinhamento com as diretrizes corporativas da instituição.

DO COMITÊ DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

I. Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, nomeados para participar do grupo pelo período de um ano;

II. A composição mínima deve incluir um colaborador de cada uma das áreas: TI, Operacional, Obras, DP, DH, Financeiro, Fiscal, Marketing, Comercial, Jurídico, e diretoria Executiva;

III. Exigir do Gerente de Tecnologia reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a SGS POLÍMEROS;

IV. O Comitê de Privacidade e Segurança da Informação ou sob a orientação do DPO, poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico;

V. Cabe ao Comitê de Privacidade e Segurança da Informação e/ou ao Gerente Tecnologia:

(a) Propor investimentos relacionados à privacidade e segurança da informação com o objetivo de reduzir mais os riscos;

(b) Propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;

(c) Avaliar os incidentes de segurança e propor ações corretivas;

(d) Definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.

7. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE.

I. Para garantir as regras mencionadas neste PSI, bem como de sua versão, a SGS POLÍMEROS poderá 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 poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

II. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, poder de polícia, solicitação do gerente (ou superior) ou por determinação do Comitê de Privacidade e Segurança da Informação;

III. Realizar, a qualquer tempo, inserção física (de dispositivos com alta de armazenamento) nas máquinas de monitoramento sua propriedade;

IV. Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

8. CORREIO ELETRÔNICO.

I. O objetivo desta norma é informar aos colaboradores da SGS POLÍMEROS quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

II. O uso do correio eletrônico da SGS POLÍMEROS é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a SGS POLÍMEROS e também não cause impacto no tráfego da rede.

III. Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da SGS POLÍMEROS para:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a SGS POLÍMEROS ou suas unidades vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da SGS POLÍMEROS estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que:
    - Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses SGS POLÍMEROS;
    - Contenha ameaças eletrônicas, como: RSam, mail bombing, vírus de computador;
    - Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
    - Vise obter acesso não autorizado a outro computador, servidor ou rede;

- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise burlar qualquer sistema de segurança;
- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet)
- Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Contenha perseguição preconceituosa baseada em religião, sexo, raça, cor, incapacidade física ou mental ou outras situações protegidas;
- Tenha fins políticos locais ou do país (propaganda política);
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.
- Dados Identificáveis e (ou) sensíveis de qualquer meio físico e (ou) do (CRM - Customer Relationship Management e do ERP (Sistema Integrado de Gestão Empresarial), sem autorização da alta direção e (ou) comitê de privacidade.

▪ As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador.
- Gerência ou departamento.
- Nome da empresa.
- Telefone(s).
- Correio eletrônico.

9.INTERNET.

I. Todas as regras atuais da SGS POLÍMEROS visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

II. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a SGS POLÍMEROS, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

III. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

IV. A SGS POLÍMEROS, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será considerada como inadequada, e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

V. A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades.

VI. Como é do interesse da SGS POLÍMEROS que seus colaboradores estejam bem-informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

VII. Somente os colaboradores que estão devidamente autorizados a falar em nome da SGS POLÍMEROS para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

VIII. Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

IX. É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

X. Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades na SGS POLÍMEROS e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela GESTÃO.

XI. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela Gerência de Sistemas.

XII. Os colaboradores não poderão em hipótese alguma utilizar os recursos da instituição para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

XIII. O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores, precisam ser criados a fim de viabilizar esse acesso essencial. Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca às atividades de cursos relacionados ao desenvolvimento de jogos.

XIV. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário essencial e seus integrantes definidos pelos respectivos gestores.

XV. Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado à SGS POLÍMEROS ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

XVI. Os colaboradores não poderão utilizar os recursos da SGS POLÍMEROS para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, RSam, assédio, perturbação ou programas de controle de outros computadores.

XVII. O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e, redes sociais e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea (Skype, WhatsApp e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente à Gerência de Sistemas.

XVIII. Não é permitido acesso a sites de proxy.

10. IDENTIFICAÇÃO.

I. Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a SGS POLÍMEROS e/ou terceiros.

II. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

III. Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

IV. Todos os dispositivos de identificação utilizados na SGS POLÍMEROS, tais como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

V. O usuário vinculado a tais dispositivos identificadores será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

VI. Todo e qualquer dispositivo de identificação corporativo e (ou) pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

VII. Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a SGS POLÍMEROS e a legislação (cível e criminal) será dos usuários que dele se utilizarem.

VIII. É proibido o compartilhamento de login para funções de administração de sistemas.

IX. O Departamento de Recursos Humanos da SGS POLÍMEROS é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

X. A Gerência de Sistemas responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

XI. Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas.

XII. Os usuários que não possuam perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

XIII. Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

XIV. 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 e/ou confiados.

XV. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras. Indica-se a combinação alternada de letras e números, maiúsculas e minúsculas. Indica-se o comprimento mínimo de 8 dígitos.

XVI. Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a Gerência de Sistemas SGS POLÍMEROS deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

XVII. Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

XVIII. A periodicidade máxima para troca das senhas é 90 dias (três meses), não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 30 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

XIX. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários ou por interesse da SGS POLÍMEROS. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

XX. Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

11. COMPUTADORES E RECURSOS TECNOLÓGICOS.

1. Os equipamentos disponíveis aos colaboradores são de propriedade SGS POLÍMEROS, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências ressonáveis.
2. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Gerência de Sistemas da SGS POLÍMEROS, ou de quem este determinar. As gerências que necessitarem fazer testes deverão solicitá-los previamente à Gerência de Sistemas e/ou à Gerência de Materiais e Serviços, ficando ressonáveis jurídica e tecnicamente pelas ações realizadas.
3. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.
4. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamados.
5. A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.
6. Arquivos pessoais e/ou não pertinentes ao negócio da SGS POLÍMEROS (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses

arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

7. Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.
8. Os colaboradores da SGS POLÍMEROS e (ou) detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Gerência de Sistemas.
9. No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

(a) Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Gerência de Sistemas da SGS POLÍMEROS, que terá acesso a elas para manutenção dos equipamentos;

(b) Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador;

(c) É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Gerência de Sistemas da SGS POLÍMEROS ou por terceiros devidamente contratados para o serviço.

(d) É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

(e) O colaborador deverá manter a configuração do equipamento disponibilizado pelo SGS POLÍMEROS, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.

(f) Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

(g) Todos os recursos tecnológicos adquiridos pela SGS POLÍMEROS devem ter imediatamente suas senhas padrões (default) alteradas.

(h) Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

10. Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da SGS POLÍMEROS.

(i) Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

(j) Burlar quaisquer sistemas de segurança.

(k) Acessar informações confidenciais sem explícita autorização do proprietário.

(l) Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

(m) Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

(n) Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

(o) Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

(p) Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

12. DISPOSITIVOS MÓVEIS.

I. A SGS POLÍMEROS deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis.

II. Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Gerência de Sistemas, como: notebooks, smartphones e pendrives.

III. Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

IV. A SGS POLÍMEROS, na qualidade de proprietária dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

V. O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na SGS POLÍMEROS, mesmo depois de terminado o vínculo contratual mantido com a instituição.

VI. Todo colaborador deverá UTILIZAR SEU DISPOSITIVO MÓVEL (pessoal ou corporativo) sob a Política BYOD a ser acordada pela SGS POLÍMEROS, sempre sob uma solução do tipo container que garanta a privacidade do colaborador e garanta a proteção dos dados da organização, exemplo: SOPHOS com EDR e outros.

VII. O suporte técnico aos dispositivos móveis de propriedade da SGS POLÍMEROS e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

VIII. Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel. Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da Gerência de Sistemas.

IX. O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da Gerência de Sistemas da SGS POLÍMEROS.

X. A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante, sujeitando o infrator às penas da lei.

XI. É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

XII. É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela SGS POLÍMEROS, notificar imediatamente seu gestor direto e a Gerência de Sistemas. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

XIII. O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a ciência e responsabilização de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à SGS POLÍMEROS ou a terceiros.

XIV. O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede do SGS POLÍMEROS deverá submeter previamente tais equipamentos ao processo de autorização da Gerência de Sistemas.

XV. Equipamentos portáteis, como smartphones, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão na rede corporativa, salvo se autorizados via Firewall e (ou) Política BYOD. O uso sem política BYOD estabelecida de dispositivos particulares (de propriedade do colaborador), não caracteriza jornada extra de trabalho e (ou) trabalho após o horário de expediente, salvo se acordado de forma diversa pela SGS POLÍMEROS mediante contrato de trabalho específico.

XVI. Expressamente em relação aos colaboradores da SGS POLÍMEROS: não obstante a permissão de dispositivos móveis ainda que não fornecidos pela instituição e/ou mesmo que utilizem redes próprias de navegação tais como 3G, 4G, quando dentro do espaço

geográfico da instituição, é terminantemente proibido o acesso a sites de conteúdo pornográfico ou criminoso.

13. DATACENTER.

I. O acesso ao Datacenter somente deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético entre outros.
II. Todo acesso ao Datacenter, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio.
III. Deverá ser executada semanalmente uma auditoria nos acessos ao Datacenter por meio do relatório do sistema de registro.
IV. O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do coordenador de infraestrutura, de acordo com o Procedimento de Controle de Contas Administrativas.
V. A lista de funções com direito de acesso ao Datacenter deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Datacenter, e salva no diretório de rede.
VI. Nas localidades em que não existam colaboradores da área de tecnologia da informação, pessoas de outros departamentos deverão ser cadastradas no sistema de acesso para que possam exercer as atividades operacionais dentro do Datacenter, como: acionamento ou desligamento de ar condicionado, suporte em eventuais problemas, e assim por diante.
VII. O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado, que deverá preencher a solicitação de acesso prevista no Procedimento de Controle de Acesso ao Datacenter, bem como assinar o Termo de Responsabilidade.
VIII. O acesso ao Datacenter, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por exemplo em casos de incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

IX. Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração de liberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao Datacenter.

X. Deverão existir duas cópias de chaves da porta do Datacenter. Uma das cópias ficará de posse do coordenador responsável pelo Datacenter, a outra, de posse do coordenador de infraestrutura.

XI. O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

XII. Não é permitida a entrada de nenhum tipo de alimento, bebida, ou produto inflamável.

A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Datacenter, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos.

XIII. No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de colaboradores autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao Datacenter.

14. BACKUP.

I. Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

II. Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto,

ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

III. As mídias de backup (como NAS e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

IV. As unidades de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

V. O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante. É necessário da mesma forma, que logs de algoritmo de integridade HASH sejam acompanhados através de relatórios emitidos pela área responsável.

VI. É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

VII. Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

VIII. É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Procedimento de Controle de Mídias de Backup.

IX. As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de sala-cofre, distante no mínimo 2 quilômetros do Datacenter.

X. Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios da SGS POLÍMEROS, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

XI. Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

XII. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Controle de Backup e Restore.

XIII. Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup.

XIV. Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

XV. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

XVI. Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador de infraestrutura, nos termos do Procedimento de Controle de Backup e Restore.

XVII. Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

15. MONITORAMENTO E IMAGENS DE SEGURANÇA.

I. A empresa SGS POLÍMEROS possui a prerrogativa de monitorar todas as dependências que compõem a organização através de câmeras de monitoramento que armazenam imagens pelo período de 30 dias com o intuito de atender à legislação vigente (Toma-se como base legal o artigo 11 (I), itens (a,b, d, e,g), e §2, da Lei 13.709/2018.). O armazenamento periódico deve ser referenciado (tempo de armazenamento x substituição de novos registros x cópias de segurança x mecanismos físicos e lógicos de proteção), e

para cumprir com as premissas de segurança patrimonial e pessoal de todos os colaboradores.

II. O acesso às imagens só poderá ser realizado pelos seguintes agentes desde que em legítimo interesse da organização:

a) Pela área de Tecnologia e Informação;
b) Pela equipe de Segurança;
c) Pela diretoria ou setor jurídico da organização;
d) Pelos gestores das demais áreas desde que acompanhados pelo jurídico ou diretoria da instituição.

III. Toda e qualquer imagem resgatada do sistema de vigilância só poderá ser disponibilizada à terceiros desde que sob medida de segurança ou autorização judicial devidamente expedida pelas autoridades competentes e atreladas à legislação do estado/município local.

16. CONTROLE DE ACESSO FÍSICO.

I. O acesso sem permissão a áreas que contenham informações sensíveis de colaboradores ou de classificação confidencial, restrita, ou privada, torna-se expressamente proibida sem a devida autorização do gestor responsável.

II. Entre as áreas que necessitam de autorização de acesso enumeram-se:

a) Sala da diretoria;
c) Sala do departamento de tecnologia e informação (TI);
d) Sala do departamento Fiscal;
f) Sala do departamento jurídico;
g) b) Sala do departamento de recursos e (ou) desenvolvimento humano;
i) Sala de segurança/monitoramento;
k) Sala de Obras e projetos;
n) depósitos sob supervisão de CG atrelada.

III. O acesso sem autorização a qualquer departamento sem o devido consentimento do gestor responsável, torna-se passível de advertência grave.

17. LGPD – TRATAMENTO DE DADOS IDENTIFICÁVEIS E (OU) SENSÍVEIS DOS COLABORADORES:

I. Trata-se da declaração de tratamento de informações (dados identificáveis e (ou) sensíveis) dos colaboradores internos e (ou) contratados por parte da SGS POLÍMEROS. A aceitação e ciência deste termo providenciada pelo colaborador mediante assinatura de próprio punho ou através de assinatura digital viabilizada por uma "ACT", torna legítima a comunicação expressa providenciada pela SGS POLÍMEROS ao Colaborador no ato de sua contratação, referente ao modo de tratamento de informações identificáveis e (ou) sensíveis, e aplica-se, a base legal do tipo "Consentimento" por parte do colaborador, para o tratamento específico destas informações para a execução de políticas públicas e cumprimento das normativas e legislações vigentes no território Nacional (Brasil), conforme as determinações legais estabelecidas em cada Estado e município do nosso país, sendo considerada a (LGPD – Lei 13.709/2018) como a lei de tratamento de informações identificáveis e (ou) sensíveis de titulares.

II. Fica estabelecido que as medidas necessárias para reduzir os riscos até os níveis aceitáveis de tratamento são promovidas em consonância com os requisitos da ISO/IEC 27001 e 27701, para promover o nível máximo de proteção conforme a capacidade da organização, o que não enfatiza a declaração de "total garantia de proteção de informações" por parte da SGS POLÍMEROS. Desde já, toma-se como norteamento, a última declaração de aplicabilidade assinada pela alta direção, para ratificar o compromisso de salvaguarda, proteção e controles aplicados para garantir a confidencialidade, a integridade e a disponibilidade das informações coletadas, processadas, e armazenadas pelo tempo estabelecido pelas normativas e leis associadas ao ciclo de vida de informações dos setores de Recursos Humanos, Departamento Pessoal, e Desenvolvimento Humano.

III. Estão associadas a este modelo de tratamento, informações dos tipos:

• banco de currículos (Observar Processo específico indicando tempo de armazenamento e modo de descarte);

• dados fornecidos à seguradora do plano de saúde e seguro de vida (Observar contrato e cláusulas de tratamento de informações pela Seguradora – A empresa Contratante (SGS POLÍMEROS) torna-se OPERADORA DE DADOS, e assume corresponsabilidade no modo de tratamento, fazendo-se necessário apontar precisamente qual é a empresa operadora parceira e disponibilizar sua política de privacidade e segurança;

• dados compartilhados com a empresa responsável por fechar folha de pagamento (Observar responsabilidade solidária e mecanismos seguros de tratamento – faz-se necessário apontar precisamente quais são as empresas que operam dados em nome do controlador e para qual atividade específica). Da mesma forma, faz-se necessário disponibilizar sua política de privacidade e segurança;

• envio de dados para o sindicato, associações de classe e órgãos públicos; pagamento (Observar responsabilidade solidária e mecanismos seguros de tratamento - faz-se necessário apontar precisamente quais são as empresas que operam dados em nome do controlador e para qual atividade específica, incluindo o número para contato). Da mesma forma, faz-se necessário disponibilizar sua política de privacidade e segurança;

• exames admissionais - – faz-se necessário apontar precisamente quais são as empresas que operam dados em nome do controlador e para qual atividade específica, incluindo o número de contato). Da mesma forma, faz-se necessário disponibilizar sua política de privacidade e segurança;

18. POLÍTICA BYOD – BRING YOUR OWN DEVICE – PARA COLABORADORES INTERNOS/EXTERNOS:

I. A SGS POLÍMEROS, estabelece as diretivas a serem cumpridas mediante a utilização de dispositivos corporativos e (ou) particulares para a realização de tarefas subordinadas às

funções que exijam comunicação e (ou) transferência de arquivos digitais através de Dispositivos Informáticos (Notebooks, Smartphones, Tablets etc.) (Obs. Destacar no termo de Contratação e (ou) contratos de prestação de serviços.)

II. Fica estabelecido que é terminantemente proibida a veiculação de imagens e (ou) documentos que contenham dados identificáveis e (ou) sensíveis, através de grupos de comunicação interna/externa, que não tenham sido expressamente autorizados e (evidenciados) pelos titulares dos dados previamente. Fotos a partir de celulares ou outros dispositivos de captura de imagens, poderão ser promovidas apenas nos seguintes casos:

a) Tenham sido coletados os termos específicos de autorização para utilização e (ou) veiculação de dados (sensíveis) onde o titular dos dados, seja parte integrante da ação;

b) Os canais de utilização estejam expostos no documento de autorização de forma explícita ex: whatsApp, redes sociais etc;

c) Não existam outras possibilidades de utilização e (ou) veiculação de conteúdo sensível, que não tenham sido previamente declaradas, autorizadas, e evidenciadas pelo agente coletor.

III. Torna-se necessário, que mediante a utilização de dispositivos de comunicação digital particulares pelos colaboradores internos em regime CLT, sejam acordados no termo de contratação, e estejam sob a gerência da área jurídica observando as questões trabalhistas relacionadas ao desempenho das funções e jornadas de trabalho. É altamente recomendável, que mediante a aceitação deste cenário, a organização providencie soluções que garantam a privacidade e a segurança das informações tanto do colaborador quanto da organização, como por exemplo, soluções SOPHOS que providenciem containers gerenciados pela área de tecnologia, e da mesma forma, possam inibir a utilização de recursos associados á organização, fora do horário acordado entre a contratante e o contratado.

19. DAS DISPOSIÇÕES FINAIS.

I. Assim como a ética, a segurança da Informação deve ser entendida como parte fundamental da cultura interna da SGS POLÍMEROS, ou seja, qualquer incidente de segurança subentende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

São Sebastião do Cai/RS, 19 de março de 2024.

Assinado digitalmente por:
NEI EDUARDO SCHNEIDER
CPF: ***.815.350-**
Certificado emitido por AC PLANO DIGITAL CD
Data: 19/03/2024 13:35:59 -03:00

IDeiaSigner

Nei Eduardo Schneider

Diretor

Assinado digitalmente por:
LUIS CARLOS MOUTINHO GARCIA
CPF: ***.516.180-**
Certificado emitido por AC CNDL RFB v3
Data: 19/03/2024 13:38:03 -03:00

IDeiaSigner

Luis Carlos Moutinho Garcia

DPO

MANIFESTO DE ASSINATURAS

Código de validação: AFZD8-ZZ5CC-PGHJH-CXSXY

Esse documento foi assinado pelos seguintes signatários nas datas indicadas (Fuso horário de Brasília):

- NEI EDUARDO SCHNEIDER (CPF ***.815.350-**) em 19/03/2024 13:35 - Assinado com certificado digital ICP-Brasil
- LUIS CARLOS MOUTINHO GARCIA (CPF ***.516.180-**) em 19/03/2024 13:38 - Assinado com certificado digital ICP-Brasil

Para verificar as assinaturas, acesse o link direto de validação deste documento:

https://app.ideiasigner.com.br/validate/AFZD8-ZZ5CC-PGHJH-CXSXY

Ou acesse a consulta de documentos assinados disponível no link abaixo e informe o código de validação:

https://app.ideiasigner.com.br/validate