CONSTRUTORA SANT'ANNA

POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES

GSA-POL005

CERTIFICADO ISO 9001
CERTIFICADO ISO 45001
INSTITUIÇÃO SOCIALMENTE RESPONSÁVEL

santanna@gruposantanna.com.br • construtorasantanna.com.br
Rua São Pedro da Aldeia, 1200 • Bairro Pilar • Belo Horizonte - MG • CEP: 30390.000 • Tel: 31 2125 2562 • 2125 2527

ÍNDICE

1. PREFÁCIO 3

2. ESCOPO 4

3. FINALIDADE 4

4. DECLARAÇÃO DA PSI - POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES NOGRUPO SANT'ANNA (GSA) 5

4.1 AUTORIDADES E RESPONSABILIDADES 6

4.2 CLASSIFICAÇÃO DA INFORMAÇÃO 8

4.2.1 PROPRIEDADE DAS INFORMAÇÕES 8

4.2.2 NÍVEIS DAS INFORMAÇÕES 8

4.3 TRATAMENTO DE DADOS PESSOAIS 9

4.3.1 DADOS E INFORMAÇÕES EM MEIO FÍSICO / IMPRESSAS 10

4.3.2 DADOS E INFORMAÇÕES EM MEIO DIGITAL 10

4.3.2.1 GESTÃO DE SOFTWARES E ACESSOS 11

4.3.2.2 ACESSO FÍSICO AOS SERVIDORES E "APPLIANCES" 12

4.4 MONITORAMENTO DE SEGURANÇA 12

4.5 CONTROLES DE ACESSO FÍSICO E LÓGICO 13

4.6 SEGURANÇA DA INFORMAÇÕES E DADOS POR FORNECEDORES 13

4.7 REQUISITO DA PSI PARA EX-COLABORADORES/AS 14

4.8 TERMO DE RECEBIMENTO, CIÊNCIA E DE ACORDO 14

4.9 TRATAMENTO DE VIOLAÇÃO DE SEGURANÇA E PRIVACIDADE 14

5. COMUNICAÇÃO DE DESVIOS OU SUSPEITAS 15

5.1 COMITÊ DE ÉTICA 15

6. SOFTWARE DE GESTÃO DA CONFORMIDADE COM A LEI DE PROTEÇÃO DE DADOS. 15

7. DIVULGAÇÃO DA PSI E TREINAMENTOS 16

8. ANEXOS 17

9. HISTÓRICO REVISIONAL 17

1. PREFÁCIO

O valor da informação varia conforme o indivíduo interessado, as necessidades e o contexto em que ela é produzida e compartilhada. Uma informação pode ser altamente relevante para um indivíduo e ao mesmo tempo não ter significado nenhum para outro.

Logo, a segurança das informações está relacionada diretamente com a proteção das informações, no sentido de preservar o valor que elas representam aos indivíduos interessados.

Esta Política trata da segurança da informação e proteção de dados, dentro do escopo definido. Não afeta nem deve servir de justificativa para negar ou dificultar o acesso/fornecimento lícito de informações às pessoas e/ou autoridades de direito, sendo valido reafirmar os compromissos e processos da empresa/GSA em relação à transparência na governança corporativa.

Foi desenvolvida e deve ser mantida alinhada aos requisitos aplicáveis da Lei 13.709 – Lei Geral de Proteção de Dados (LGPD) e também:

- Lei 12.965 - Marco Civil da Internet;
- NBR ISO/IEC 27001;
- NBR ISO/IEC 27002;
- Boas práticas e sugestões da ANPPD - Associação Nacional de Profissionais de Privacidade de Dados;
- Condutas, Normas e Procedimentos internos, aperfeiçoados constantemente, aprovados pelas alçadas competentes e disponibilizados a todos os colaboradores.

Para facilidades gerais, serão usadas as abreviações:

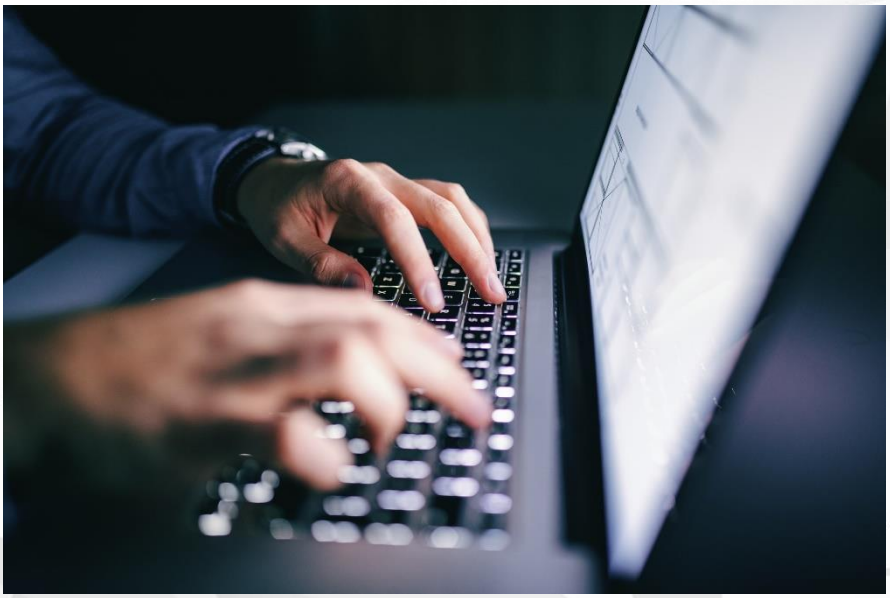
- ANPD para a Autoridade Nacional deProteção de Dados;
- GSA para Grupo Sant'Anna (www.gruposantanna.com.br).

Caso encontre palavras e termos nesta Política e/ou nos outros documentos do SGI/GSA cujas definições/conceitos sejam novos ou causem dúvidas, gentileza consultar a legislação,ou normas técnica de referência e/ou dicionários do idioma utilizado.

2. ESCOPO

As diretrizes estabelecidas nesta Política deverão ser seguidas pelos usuários e usuárias de dados e informações sejam de propriedade ou estejam sob o domínio ou responsabilidade das empresas do GSA.

Não se aplica aos dados impessoais, relativos a pessoas jurídicas, como CNPJ, razão social, endereço comercial, entre outros.



Para casos de conflitos em relação à práticas de transparência, excepcionalidades ou temas não abordados nesta Política deverão ser comunicados, analisados e deliberados pela Diretoria, com parâmetros na legislação aplicável, o Código de Ética (GSA-CEC 001) e as melhores práticas na área.

3. FINALIDADE

Estabelecer diretrizes aos usuários de informações e dados que a Empresa detém sob a sua responsabilidade, determinando:

- Os processos internos para tratamento de dados pessoais pela empresa/GSA, objetivando proteger os direitos fundamentais de liberdade e de privacidade de pessoas físicas;

- Os padrões de comportamento relacionados à segurança, proteção e privacidade de dados estratégicos, bem como demais informações necessárias ao desenvolvimento e desempenho das operações empresariais.

4. DECLARAÇÃO DA PSI - POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES NOGRUPO SANT'ANNA (GSA)

Os compromissos das empresas do GSA descritos nesta Política para proteção e privacidade de dados / segurança das informações se baseiam nos seguintes princípios:

- CONFIDENCIALIDADE: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- 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.
- DISPONIBILIDADE: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Sendo mandatório e primordial aos usuários e todos/as (pessoal próprio ou terceiros/as) que desenvolvem quaisquer atividades nas empresas do Grupo Sant'Anna ou em seu nome:

- Assegurar a integridade e disponibilidade das informações segundo esta Política e os requisitos aplicáveis relativos à segurança, proteção e privacidade de dados e informações;
- Assumir uma postura proativa no que diz respeito à proteção das informações, com atenção contínua para prevenir ameaças externas, bem como fraudes e acesso indevido a sistemas de informação sob responsabilidade da empresa.

Informações confidenciais, secretas e internas não devem ser expostas publicamente.
As informações recebidas pela Empresa, devem ser tratadas e armazenadas de forma segura e íntegra, como requerido.

Todos os processos da empresa e Grupo Sant'Anna que envolvem tratamento, armazenamento e transferência de dados pessoais e/ou sensíveis, sejam de beneficiários, empregados e prestadores de serviço de qualquer natureza, devem estar em conformidade com as bases legais que definem e legitimam o tratamento de dados pessoais e preservam os direitos dos titulares destes dados.

Os princípios e diretrizes gerais a serem observados e aplicados são apresentados a seguir:

4.1 AUTORIDADES E RESPONSABILIDADES

A Alta Direção designa e mantém ativos, profissionais devidamente habilitados e competentes para exercer as funções de:

RESPONSÁVEIS	DESCRIÇÃO	PRINCIPAIS ATRIBUIÇÕES / RESPONSABILIDADES
DIRETORIA SUPERINTENDENTE	Representante oficial da empresa.	Solicitar aos conselheiros a assinatura do Termo de Confidencialidade e Proteção às Informações para conselheiros. Aprovar, cumprir e fazer cumprir as diretrizes e normas desta PSI,bem como das eventuais revisões/alterações; Definir/aprovar os critérios de constituição e coordenação de Comissões ou Comitês de Segurança da Informação; Prover recursos necessários bem como autoridade requisitada àspartes envolvidas na execução e manutenção da PSI e no atendimento a legislação pertinente.
GERÊNCIA ADMISTRATIVO-FINANCEIRA (GAF)	Autoridade quefaz gestão dosserviços administrativos e financeiros na empresa/GSA	Definir, organizar, implantar e manter a eficácia da regras necessárias para salvaguarda requerida das informações - videesta PSI, PS009 e demais normas internas e leis relacionadas; Definir e apoiar estratégias necessárias à implantação e manutenção da Política de Proteção de Dados; Validar e propor ajustes, aprimoramentos e modificações destaPolítica e demais normas de segurança da informação, submetendo a aprovação da Diretoria; Manter a atualização/aplicação dos conceitos de classificação das informações pertencentes ou sob a guarda da empresa e acessos a serem aplicados pelos usuários nas suas atividades; Notificar as partes interessadas sobre os casos de violação daPolítica e das normas de segurança da informação; Assegurar que violações da PSI, normas e leis de segurança das informações sejam recebidas/documentas, analisadas e tratadas, com devidos encaminhamentos à Diretoria e/ou Comitê de Ética; Deliberar sobre os temas relacionados à segurança da informação, privacidade e proteção de dados pessoais reportados. Determinar criação de "Comissões ou Comitês" de Segurança da Informação, sempre que precisar de apoio ou para analisar e deliberar sobre pautas/temas multidisciplinares. Definir criação, escopo e trâmites das Comissões/Comitês de Segurança da Informação, quando houver, assegurando seu funcionamento e eficácia. Autorizar uso de câmeras fotográficas, filmadoras e smartphonepara fotografar ou filmar dados e informações não públicas (confidenciais, restritas e internas) – salvo casos 4.5.

SETOR DE TECNOLOGIA DA INFORMAÇÃO (STI)E DESIGANDOS.	Pessoal que disponibiliza e cuida dos assuntos de TIda empresa conforme PS009.	Manter a adequação dos recursos de TI frente aos requisitos dalegislação pertinente, desta Política e também do PS009; Auxiliar no processo de revisão e atualização da Política de Segurança da Informação quando necessário; Fazer parte dos Comitê/Comissão de Segurança da Informação; Disponibilização do portal GestãoX-LGDP®, pra as partes, bem como gestão das rotinas de alimentação/retroalimentação doportal.

DPO (*Data ProtectionOfficer)*	Pessoa devidamente indicado pelo/a Controlador e pelo/a Operador/a	Manter/assegurar a proteção de dados, devidamente indicado pelo/a Controlador e pelo/a Operador/a para atuar como canal decomunicação entre o Controlador, os titulares dos dados e a ANPD.
SETOR DE RECURSOS (SRH) ADMINISTRATIVO DE OBRAS (ADO)	Pessoal responsável pelo recrutamento, seleção e integração do pessoal.	Prover treinamentos a todos os envolvidos nesta Política; Divulgar as diretrizes estabelecidas nesta Política através dosmeios oficiais de comunicação da empresa.
DEPARTAMENTO PESSOAL (DP) ADMINISTRATIVO DE OBRAS (ADO)	Pessoal responsável pela contrataçãoe administração da folha de pessoal.	Solicitar aos usuários a assinatura e reter registro dos termos ou clausulas de confidencialidade e proteção às informações para Colaboradores.
RLST (RESPONSÁVEIS PELAS LOCAÇÕES E SERVIÇOS DE TERCEIROS) ADMINISTRATIVO DE OBRAS (ADO) GTC (Gestão deContratos)	Pessoal encarregado pelas locações e/ou contratações de serviços de terceiros e administração dos contratos.	Atribuir aos Usuários, na fase de contratação e de formalização dos contratos, de prestação de serviço ou individuais de trabalho,a responsabilidade do cumprimento desta Política; Solicitar aos usuários a assinatura e reter registro dos termos ou clausulas de confidencialidade e proteção às informações dos Prestadores de Serviços.
USUÁRIOS	Todos/as que exerçam atividades na ou para a empresa.	Observar as regras e diretrizes desta Política, zelando continuamente pela proteção de dados e informações contra acesso, modificação, destruição ou divulgação não autorizada; Comunicar aos canais oficiais de Ouvidoria ou da Comissão de Ética, quaisquer atos ou suspeitas de violação às legislações enormas internas; Propor melhorias à segurança da informação e privacidade dedados na/da empresa/GSA.

NOTA: No âmbito desta Política, entende-se por USUÁRIOS/USUÁRIAS todas pessoas, físicas ou jurídicas, que exerçam atividades para a empresa/GSA ou esteja a seu serviço. Ex.: colaboradores, administradores (Diretores e Gestores), comitês e grupos de trabalho, assessorias, prestadores de serviço, etc.

4.2 CLASSIFICAÇÃO DA INFORMAÇÃO

Toda a informação de propriedade da Empresa ou sob sua responsabilidade deve ser classificadas para possibilitar o controle adequado, podendo ser:

4.2.1 PROPRIEDADE DAS INFORMAÇÕES

INFORMAÇÕES PERTENCENTES AOS USUÁRIOS: dados externos, apenas manipuladas ou armazenadas nos meios pelos quais a empresa/GSA detém controle administrativo, físico, lógico e responsabilidade legal.

INFORMAÇÕES DE PROPRIEDADE DA EMPRESA: todas as criações, códigos ou procedimentos desenvolvidos por qualquer administrador, colaborador ou prestadores de serviço de qualquer natureza durante todo o seu vínculo com a Empresa.

4.2.2 NÍVEIS DAS INFORMAÇÕES

CLASSIFICAÇÃO DAS INFORMAÇÕES	
NIVEL	**ESPECIFICAÇÃO**
PÚBLICA	Informações que podem ser divulgadas sem restrições para todos os públicos, interna e externamente, sem gerar indevidamente nenhum impacto negativo às partes afetadas.
INTERNA	Informações de interesse e uso exclusivamente interno. Não devem ser expostas externa e/ou publicamente.
RESTRITA	Informações da empresa, tais como dados técnicos, comerciais, etc. Só podem ser usadas por grupos, áreas de negócio ou cargos específicos da empresa.
CONFIDENCIAL	São informações protegidas por lei e por órgãos reguladores, de caráter pessoal dos titulares, cláusulas de confidencialidade, do quadro corporativo e/ou informações estratégicas para os negócios/empresas. Logo, também são consideradas confidenciais: informações sobre os colaboradores, registros financeiros e contábeis; documentação relativa a propostas técnicas e comerciais, inovações e novos negócios; negociações, contratos e acordos comerciais; relatórios e diagnósticos internos de qualquer natureza; pesquisas, estudos, planosde ação e decisões estratégicas. Devem restrita a um grupo específico de pessoas. A divulgação não autorizada e/ou indevida dessas informações pode causar impactos de ordem financeira, legal, normativa, contratual, operacional, estratégica,danos à imagem e reputação da empresa ou ainda sanções administrativas, cíveis ou criminais.

4.3 TRATAMENTO DE DADOS PESSOAIS

Deve ser garantida segurança dos dados pessoais tratados pela Empresa.

Os dados e informações pessoais tratados devem ser coletados de forma ética, com o conhecimento do titular e para propósitos específicos;

São devidamente tomadas as medidas razoáveis para garantir que os dados dos titulares sejam tratados dentro da necessidade, apoiados nas bases legais pertinentes;

Deve-se minimizar os dados, limitados ao que é necessário em relação aos propósitos para os quais serão processados.

O compartilhamento de dados pessoais ou sensíveis com terceiros, somente poderá ser feito em consonância com esta Política e em conformidade com as atividades de tratamento de dados pessoais.

Todos os dados coletados serão mantidos enquanto o cadastro do titular estiver ativo e conforme seja necessário para as atividades da empresa, observando os períodos de retenção estabelecidos em contrato, em outras leis ou requisitos específicos, se houver, que suporte a retenção.

Descarte de dados pessoais feito com segurança, de forma que os dados sejam irrecuperáveis.

Usuários/as inseguros/as ou com dúvidas em relação aos cuidados e procedimentos corretos para aquisição, uso ou descarte dessas informações devem buscar orientação junto ao DPO ou da Administração da empresa.

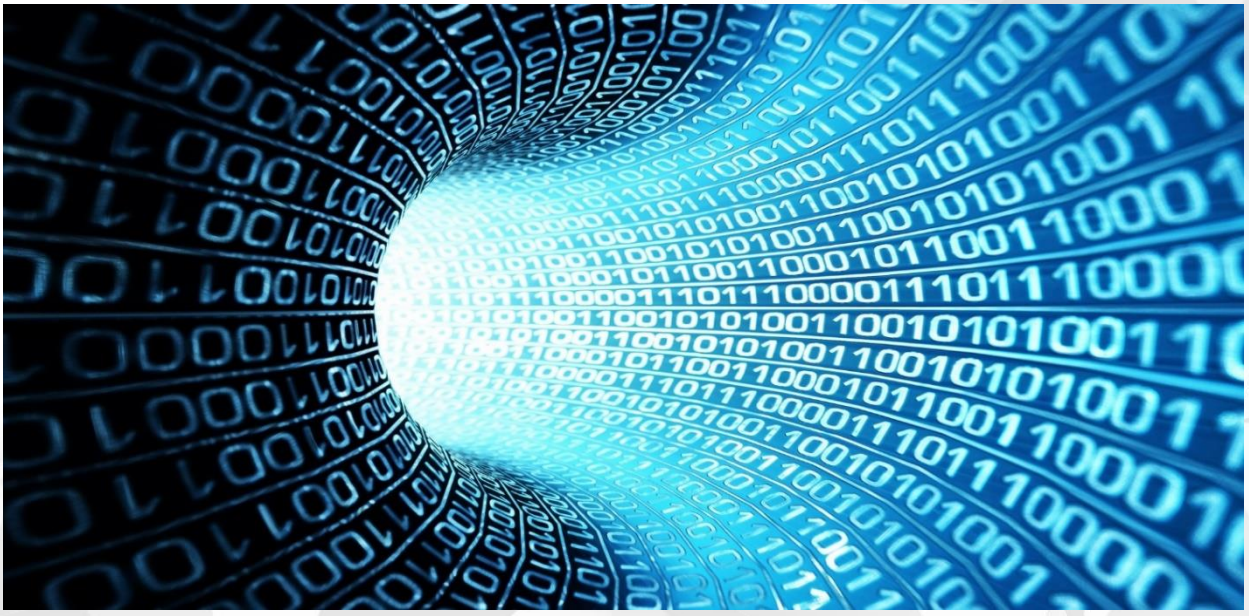
4.3.1 DADOS E INFORMAÇÕES EM MEIO FÍSICO / IMPRESSAS

Documentos impressos e arquivos contendo dados pessoais e/ou informações confidenciais, secretas e internas devem ser armazenados e descartados de forma segura, conforme descrito nesta Política e outras normas da empresa – Ver PS010,item Programa Sou Mais Sant'Anna.

4.3.2 DADOS E INFORMAÇÕES EM MEIO DIGITAL

Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às devidas permissões de acesso (item 4.3.2.1).

Qualquer informação ou documento corporativo somente poderá ser armazenado em bancos de dados, internos ou em "nuvem", administrados e\ou homologado (aceito/definido) pelo STI da empresa/GSA.



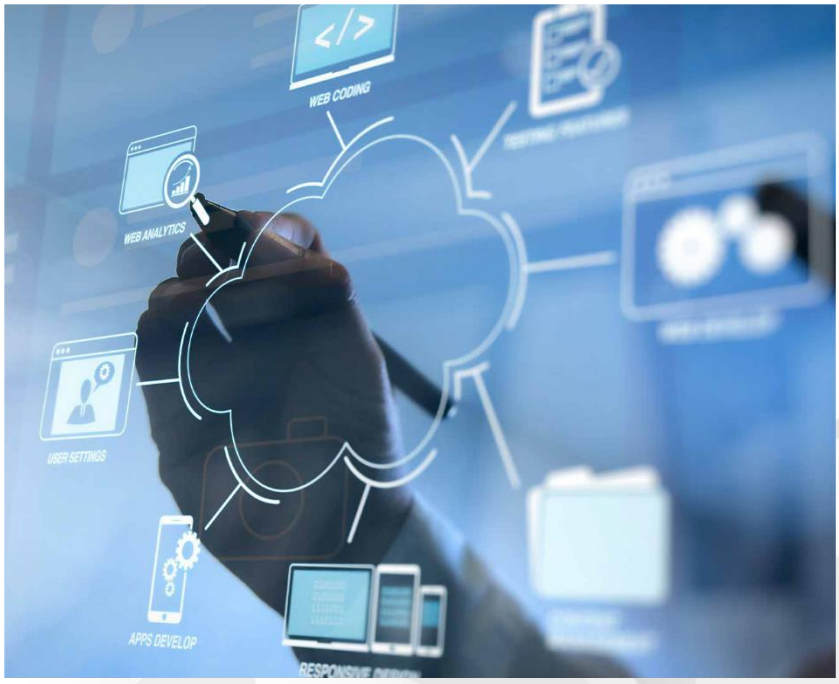
Utilizamos mecanismos de segurança tecnológica e administrativa suficientes para proteger todos os dados e informações armazenadas, nos termos estabelecidos na Lei Geral de Proteção de Dados e outros requisitos aplicáveis. Logo, todos os dados inerentes à empresa são mantidos protegidos por meio de rotinas sistemáticas, documentadas, com cópia de segurança, devendo ser submetidos a testes periódicos de recuperação. Nota: Os meios e responsabilidades para realização e manutenção dos processos de backups estão definidos no PS009 – TI.

4.3.2.1 GESTÃO DE SOFTWARES E ACESSOS

Os softwares corporativos poderão ser utilizados no ambiente da Empresa, somente após homologação do responsável pelo STI e validação do DPO, caso aplicável.

De acordo com as regras de permissão de acesso, para aqueles que não tiverem autorização definida, as cópias de qualquer informação ou documento corporativoem dispositivos removíveis, tais como pen drive, HD externo e itens da mesma categoria, deverão ser previamente autorizadas pelo responsável pela Segurança daInformação.

Manutenção pelo STI da empresa, de avaliação, monitoramento e gerenciamentos das permissões de usuários, administradores e desenvolvedores, considerando a necessidade de acesso a cada nos Banco de Dados, aplicando essas permissões de acesso aos usuários de maneira adequada aos serviços realizados;



O acesso lógico aos sistemas computacionais, disponibilizados pela Empresa, deve ser controlado, garantindo a rastreabilidade e a efetividade do acesso autorizado, salvo os acessos de conteúdo de caráter público.

Todo usuário deverá possuir chave e senha previamente cadastrados, sendo esta, pessoal e intransferível, sendo proibida a utilização de códigos de acesso genéricos ou comunitários, exceto quando devidamente autorizado pelo gerente imediato e pelo Gerente de Tecnologia da Informação, por meio de registro de chamado.

Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados, exceto quando devidamente autorizados.

Nenhum usuário deve ter, por padrão, acesso de "Administrador" em estações de trabalho e/ou notebooks. Caso seja necessário tal acesso, deverá ser feita uma solicitação a área responsável por meio de abertura de chamado par o STI, com a devida finalidade destacada para avaliação e poderão ser autorizadas ou negadas.

NOTA: O padrão interno PS009 - Tecnologia da Informação, detalha os requisitos e responsabilidades dos elementos de gestão de softwares e acessos citados acima.

4.3.2.2 ACESSO FÍSICO AOS SERVIDORES E "APPLIANCES"

O acesso físico aos servidores e "appliances" são autorizados apenas ao pessoal doSTI do GSA ou à autorizados/as por ele (STI), quando justificável.

Todo acesso à servidores e "appliances" deve ser registrado de forma manual ou automatizada em sistema de controle de acesso. Os registros de acesso devem ser armazenados em local seguro e mantidos conforme procedimento do STI (PS009).

No caso de auditorias nos servidores e "appliances", o acesso somente será autorizado se um/a representante do STI da empresa acompanhar/supervisionar à equipe auditora, do início ao fechamento dos trabalhos.

Para terceiros realizarem serviços em servidores e "appliances" será necessária a aprovação e também o acompanhamento/supervisão devida, dos líderes do STI.

4.4 MONITORAMENTO DE SEGURANÇA

Visando garantir as regras de segurança, a Empresa monitora periodicamente seus processos e sistemas de informação, considerando os procedimentos apresentados a seguir:

- Uso de sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e componentes da rede, possibilitando, quando pertinente, identificar usuários e respectivos acessos efetuados, bem como material manipulado;

- São feitas inspeções físicas nas máquinas sob domínio da empresa;
- Uso de sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações, do ambiente de infraestrutura e dos perímetros de acesso;
- Periodicamente são realizados testes de vulnerabilidade (mínimo semestral).

4.5 CONTROLES DE ACESSO FÍSICO E LÓGICO

Não é permitido o compartilhamento de dados pessoais e sensíveis dentro e fora das dependências da empresa/GSA por qualquer meio de comunicação, que não seja para o exercício profissional.

As informações e dados restritos e confidenciais da empresa podem ser disponibilizados às empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento desta PSI e de todas as diretivas de segurança e privacidade de dados, formalizado por meio de contratos com cláusulas sobre o assunto e/ou da assinatura do ANEXO GSA-POL005/2 TERMO DE CONFIDENCIALIDADE E PROTEÇÃO ÀS INFORMAÇÕES PARA PRESTADORES DE SERVIÇO.

Os dados e informações devem ser acessados somente por pessoas autorizadas ecapacitadas para que o uso seja adequado. Além disso, o acesso deve ser específico e restrito à necessidade de execução da sua atividade - ver item 4.3.2.1.

Não é permitido envio de informações ou documentos corporativos para e-mails pessoais de colaboradores ou de terceiros.

Para acesso às dependências da empresa, deve ser observado e seguido o procedimento interno especifico - PS008 Serviços Compartilhados.

É proibida a utilização de câmeras fotográficas, filmadoras, smartphone e outros, para fotografar ou filmar dados e informações classificadas como confidenciais, secretas e internas para divulgação ou compartilhamento com terceiros, em qualquer uma das dependências da empresa salvo em situações inerentes à rotina de trabalho, previamenteautorizadas (ver item 4.1) e/ou situações de emergência, se requerido.

4.6 SEGURANÇA DA INFORMAÇÕES E DADOS POR FORNECEDORES

Cláusulas contratuais devem ser estabelecidas com prestadores de serviço, contendo os procedimentos de segurança que devem ser cumpridos para proteger a confidencialidade, segurança e integridade dos dados.

Esses fornecedores também são qualificados previamente e devem manter-se em conformidade com a legislação de proteção de dados vigente.

4.7 REQUISITO DA PSI PARA EX-COLABORADORES/AS

A responsabilidade pela segurança e proteção de dados e informações por ex- colaborador estende-se pelo período mínimo de vinte e quatro (24) meses após o desligamento ou fim do contrato/prestação de serviço.

4.8 TERMO DE RECEBIMENTO, CIÊNCIA E DE ACORDO

Esta política contém o Anexo GSA POL005/1 - TERMO DE RECEBIMENTO, CIÊNCIA E DE ACORDO, onde todos usuários/as de dados e informações da Empresa/GSA ou sob sua responsabilidade deverão assinar, física ou digitalmente.

Cópias destes Termos devem ser mantidas no DP e/ou TI para consultas futuras.

4.9 TRATAMENTO DE VIOLAÇÃO DE SEGURANÇA E PRIVACIDADE

No caso de uma violação de segurança e/ou privacidade que leve à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais e informações estratégicas, a Empresa deverá prontamente:

- Avaliar o risco para os direitos e liberdades das pessoas;
- Se apropriado, informar violações à autoridade competente e/ou o também o titular.
- Realizar as análises necessárias;
- Tomar ações corretivas suficientemente eficazes para reparar ou mitigar os efeitos/danos e sobretudo eliminar causas.

Todos incidentes deverão ser registrados pelo STI ou outro designado pela Administraçãoda empresa e ficarão devidamente disponíveis para consulta da autoridade.

5. COMUNICAÇÃO DE DESVIOS OU SUSPEITAS

Desvios ou suspeita de conduta ou infração relacionada à Segurança das Informações deve ser comunicada imediatamente ao setor/área competente da empresa ou, se preferir, à Ouvidoria da empresa, no e-mail ouvidoria@gruposantanna.com.br.

Tanto o público interno quanto externo (clientes, parceiros, comunidade, etc.) também podem fazer relatos anonimamente, através do portal de Canal de Denúncias da nossa empresa - https://app.ouvex.com.br/construtorasantanna.

A Empresa compromete-se com a não retaliação a profissionais ou a terceiros que realizarem relatos de boa-fé.

É importante que todas as informações passadas sejam verídicas. Pessoas másintencionadas que descreverem mentiras, ameaças ou inverdades que possam prejudicar a reputação de outras pessoas, interna ou externa, estarão sujeitas a medidas disciplinares administrativas e judiciais cabíveis.

Estas e outras disposições sobre o Canal de Denúncias, processos de análise, investigação e estabelecimento de medidas disciplinares estão definidas e detalhadas no documento interno específico, denominado GSA-POL004 Política CRECE.

5.1 COMITÊ DE ÉTICA

As definições e diretrizes gerais sobre o COMITÊ DE ÉTICA são tratadas no CÓDIGO DEÉTICA DE CONDUTA – consultar a versão mais recente do GSA-CEC001.

6. SOFTWARE DE GESTÃO DA CONFORMIDADE COM A LEI DE PROTEÇÃO DE DADOS.

A empresa disponibiliza e mantêm software online, adequado e especifico para gestão e tratativa de incidentes relativos à Proteção de Dados.

Trata-se do portal Gestão-X LGPD®, portal desenvolvido e mantido em conformidade com as leis de proteção de dados vigentes e homologado pela ANPPD.

A gestão, operação, alimentação/retroalimentação do portal é deste O incidente deve ser registrado pelo STI ou outro designado pela Administração da empresa, no software de Gestão e Tratativa de Incidentes GestãoX-LGPD

15.3 Será de inteira responsabilidade de cada usuário, todo prejuízo ou dano que vier a sofrer ou causar à Empresa ou a terceiros, em decorrência da não observância das diretrizes e normas estabelecidas nesta Política.

7. DIVULGAÇÃO DA PSI E TREINAMENTOS

A CSGI - Coordenação do SGI mantém a versão original atualizada e disponibilizada está Política – GSA POL 005 nos meios oficiais apropriados para consulta, a qualquer momento, pelo pessoal interno.

Outras partes interessadas também podem solicitar cópia da GSA-POL005 à CSGI ouacessá-la no site da empresa (www.construtorasantanna.com.br).

Faz parte do treinamento de integração dos colaboradores, tanto na sede quanto em obras. Os processos de treinamento são tratados no procedimento interno específico - PS002 Recursos Humanos.

Cabe a cada usuário manter-se atualizado em relação a esta Política e as normas relacionadas.

8. ANEXOS

CÓD.	TÍTULO	REVISÃO VÁLIDA	
GSA-POL005/1	Termo de recebimento, ciência e de acordo	00	30/04/2021
GSA-POL005/2	Termo de confidencialidade e proteção às informações para prestadores de serviço.	00	30/04/2021

9. HISTÓRICO REVISIONAL

REVISÕES

TP: TIPO A - PARA SIMPLIFICAR B - PARA INOVAR C - PARA CORREÇÃO D – REV. ROTINEIRA D - OUTROS

Rev.	TP	Descrição	Por	Aprovação	Data
00	D	Emissão inicial	Glaysson Alcântara Gustavo Barcelos Leamara Melo Lucas Araujo (EX) Paulo André Avelino Percibal Echeverria Rainilda Fernandes Valdelino Batista	Bruno Santana	03/05/2021