SUMÁRIO

1. DEFINIÇÕES 2
2. RESPONSABILIDADES GERAIS 3
3. OBJETIVOS 4
4. ABRANGÊNCIA 4
5. CLASSIFICAÇÃO DA INFORMAÇÃO 4
6. ARMAZENAMENTO DA INFORMAÇÃO 4
7. DADOS DOS COLABORADORES 5
8. ADMISSÃO E DEMISSÃO DE COLABORADORES / TEMPORÁRIOS / ESTAGIÁRIOS 5
9. TRANSFERÊNCIA DE COLABORADORES / TEMPORÁRIOS / ESTAGIÁRIOS 6
10. PROGRAMAS ILEGAIS 6
11. PERMISSÕES E SENHAS 6
12. COMPARTILHAMENTO DE DADOS 7
13. BACKUP (COPIA DE SEGURANÇA DOS DADOS) 7
14. CÓPIAS DE SEGURANÇA DE ARQUIVOS EM DESKTOPS 8
15. SEGURANÇA E INTEGRIDADE DOS DADOS 8
16. PROPRIEDADE INTELECTUAL 8
17. ACESSO A INTERNET 9
18. USO DO CORREIO ELETRÔNICO (E-MAIL) 10
19. NECESSIDADE DE NOVOS SISTEMAS, APLICATIVOS E EQUIPAMENTOS 10
20. USO DE DISPOSITIVOS MÓVEIS 11
21. RESPONSABILIDADE DOS GESTORES 11
22. SISTEMAS DE TELECOMUNICAÇÕES 12
23. USO DE ANTIVÍRUS 12
24. PENALIDADES 12
25. SISTEMA DE HELPDESK 13
26. TRABALHO REMOTO 14
27. TRATAMENTO DO SUPORTE DA INFORMAÇÃO 14
28. CONTROLE DE ACESSOS 15

29. CONTRATAÇÃO E MANUTENÇÃO DE EQUIPAMENTOS E SERVIÇOS 16

30. ORGANIZAÇÃO E CUIDADOS GERAIS 17

31. TRANSFERÊNCIA DE INFORMAÇÃO.....17

32. TRATAMENTO DOS DESVIOS E EXCEÇÕES À PSI 18

33. REVISÃO E ATUALIZAÇÃO:.....18

34. DO COMPROMETIMENTO DA ALTA DIREÇÃO: 18

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

BASEADO NA NORMA ABNT 21:204.01-010

A Política de Segurança da Informação, na SPG, aplica-se a todos os colaboradores, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da SPG, ou acesso a informações pertencentes à SPG. Todo e qualquer usuário de recursos computadorizados da SPG tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de TI. A violação desta política de segurança é qualquer ato que:

1. *Exponha a SPG a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.*
2. *Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.*
3. *Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.*

1. DEFINIÇÕES

Backup – Cópia de Segurança.

Servidor AD (Active Directory) – Ferramenta de gestão de acesso à rede.

NAS (Network Attached Storage) – Equipamento para Backup.

CSIRI - Comitê de Segurança da Informação e Respostas a Incidentes

PSI – Política de Segurança da Informação

2. RESPONSABILIDADES GERAIS

Atividade		Responsável
Incidentes	Dados Pessoais	Comunicação imediata ao encarregado pelo tratamento de dados pessoais (*Data Protection Officer* – DPO) que acionará o Comitê de Segurança da Informação e Respostas a Incidentes e ao Gestor da área onde ocorreu o incidente
	Informações	Setor de TI que acionará o Comitê de Segurança da Informação e Respostas a Incidentes e ao Gestor da área onde ocorreu o incidente
Deliberar sobre assuntos relacionados a Política de Segurança de Informação		Comitê de Segurança da Informação
Cumprimento dos itens desta política e uso correto e responsável dos recursos de TI		Todos que se relacionam com a **Organização**, direta ou indiretamente, desde colaboradores, terceiros e prestadores de serviços.

3. OBJETIVOS

A Política de Segurança da Informação e Privacidade (PSIP) tem por objetivo proteger a Organização das ameaças internas e externas; padronizar as ações para o uso consciente, correto e seguro das informações em si e dos recursos de processamento que lhe dão suporte; garantir que a Organização atenda à legislação vigente; assegurar a disponibilidade, integridade, confidencialidade e a autenticidade da informação necessária para a realização do negócio; assegurar a proteção dos dados pessoais em qualquer operação realizada pela Organização e seus agentes e garantir a privacidade dos titulares dos dados pessoais.

4. ABRANGÊNCIA

A Política de Segurança da Informação e Privacidade aplica-se à alta direção, colaboradores independentes do cargo, estagiários, aprendizes, prestadores de serviços, fornecedores, tanto internos quanto externos, e terceiros que utilizem os recursos de processamento das informações da SPG.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do gestor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

Conceitos:

Informação Pública: É toda informação que pode ser acessada por usuários da SPG, clientes, fornecedores, prestadores de serviços e público em geral.

Informação Interna: É toda informação que só pode ser acessada por colaboradores da SPG e prestadores de serviços são informações que possuem um grau de confidencialidade que pode comprometer a imagem da SPG.

Informação Confidencial: É toda informação que pode ser acessada por usuários da SPG e por parceiros da SPG. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da SPG ou ao negócio do parceiro.

Informação Restrita: É toda informação que pode ser acessada somente por usuários da SPG explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da SPG.

6. ARMAZENAMENTO DA INFORMAÇÃO

É o momento que a informação é armazenada/salva, seja em um banco de dados, em uma anotação de papel ou ainda em uma mídia como CD-ROM e guardada em uma gaveta, todo gestor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar, mas não se limitando, nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

7. DADOS DOS COLABORADORES

A SPG se compromete em não acumular ou manter intencionalmente Dados Pessoais de Colaboradores além daqueles relevantes na condução do seu negócio. Todos os Dados Pessoais de Colaboradores que porventura sejam armazenados serão considerados dados confidenciais. Dados Pessoais de Colaboradores sob a responsabilidade da SPG não serão usados para fins diferentes daqueles para os quais foram coletados.

Dados Pessoais de Colaboradores não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos colaboradores da SPG. Por outro lado, os colaboradores se comprometem a não armazenar dados pessoais, seus e de terceiros, em, sem limitação, dispositivos, suportes de qualquer natureza da SPG, sem prévia e expressa autorização por parte da diretoria. Mesmo que seja autorizado o armazenamento dos referidos dados, a SPG não se responsabiliza por eles, nem tampouco pelo seu conteúdo e pela segurança. Tais dados jamais poderão ser armazenados nos diretórios dos Servidores de empresa, e jamais poderão fazer parte da rotina de backup da SPG.

8. ADMISSÃO E DEMISSÃO DE COLABORADORES / TEMPORÁRIOS / ESTAGIÁRIOS

O setor de RH da SPG deverá informar ao setor de TI, toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de colaboradores, para que os mesmos possam ser cadastrados ou excluídos no sistema da SPG. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id), pelo setor de TI.

Cabe ao setor solicitante da contratação a comunicação ao setor de RH sobre as rotinas a que o novo contratado terá direito de acesso via formulário definido e em poder do RH da SPG. No caso de temporários e/ou estagiários deverá também ser informado o tempo em que ele prestará serviço a SPG, para que na data de seu desligamento possam também ser encerradas

as atividades relacionadas ao direito de seu acesso ao sistema. No caso de demissão, o setor de RH deverá comunicar o fato o mais rapidamente possível à TI, para que o colaborador demitido seja excluído do sistema.

Cabe ao setor de RH dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação da SPG. Nenhum colaborador, estagiário ou temporário, poderá ser contratado, sem ter concordado com esta política.

9. TRANSFERÊNCIA DE COLABORADORES / TEMPORÁRIOS / ESTAGIÁRIOS

Quando um colaborador for promovido ou transferido de seção ou gerência, o setor de RH deverá comunicar o fato ao Setor de TI, para que sejam feitas as adequações necessárias para o acesso do referido colaborador ao sistema informatizado da SPG.

10. PROGRAMAS ILEGAIS

A SPG respeita os direitos autorais dos programas que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos seus computadores. É terminantemente proibido o uso de programas ilegais (sem licenciamento) na SPG.

Os usuários não podem, em hipótese alguma, instalar este tipo de "software" (programa) nos equipamentos da SPG, mesmo porque somente o setor de TI tem autorização para instalação de programas previamente autorizados dentro da política de segurança da SPG. Periodicamente, o Setor de TI fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas não autorizados, estes deverão ser removidos dos computadores.

Aqueles que instalarem em seus computadores de trabalho tais programas não autorizados serão responsabilizados perante a SPG, por quaisquer problemas e/ou prejuízos causados oriundos desta ação, estando sujeitos as penalidades previstas neste documento, tópico 24. PENALIDADES.

11. PERMISSÕES E SENHAS

Todo usuário para acessar os dados da rede SPG, devera possuir um login e senha previamente cadastrados pelo setor de TI.

Quem deve fornecer os dados referentes aos direitos do usuário é o responsável direto pela sua chefia, que deve preencher uma ficha e entregá-la ao setor de RH. Quando da necessidade de cadastramento de um novo usuário para utilização da "rede", sistemas ou equipamentos de TI da SPG, o setor de origem do novo usuário deverá comunicar esta necessidade ao setor de TI, por meio de memorando ou e-mail, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

A área de TI fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada imediatamente após o primeiro acesso e, posteriormente, a cada 90 (noventa) dias. Por segurança, a área de TI recomenda que as senhas tenham sempre um critério mínimo de criação para que não sejam facilmente copiadas e não possam ser repetidas.

Todos os usuários responsáveis pela aprovação eletrônica de documentos como, sem limitação, pedidos de compra, solicitações, deverão comunicar ao Setor de TI qual será o seu substituto quando de sua ausência da SPG, para que as permissões possam ser alteradas (delegação de poderes). Quando houver necessidade de acesso para usuários externos, sejam eles temporários ou não, a permissão de acesso deverá ser bloqueada tão logo este tenha terminado o seu trabalho e se houver no futuro nova necessidade de acesso, deverá então ser desbloqueada pelo setor de TI.

12. COMPARTILHAMENTO DE DADOS

Não é permitido o compartilhamento de, sem limitação, pastas nos computadores e desktops da SPG. Todos os dados deverão ser armazenados nos Servidores da rede, e a autorização para acessá-los deverá ser concedida pelo Servidor AD (Active Directory). O setor de TI está orientado a fiscalizar periodicamente todos os compartilhamentos existentes nas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam armazenados na rede. Os compartilhamentos de impressoras devem estar sujeitos as autorizações de acesso do AD. Não é permitido na SPG o compartilhamento de dispositivos móveis como, mas não se limitando, pen drive, laptop, smatphone; o colaborador será integralmente responsável por quaisquer problemas ou prejuízos causados oriundos desta ação, estando sujeitos as penalidades previstas neste documento, tópico 24. PENALIDADES.

13. BACKUP (COPIA DE SEGURANÇA DOS DADOS)

Todos os dados da SPG deverão ser protegidos por meio de rotinas sistemáticas de Backup. Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade do Setor de TI e deverão ser feitas diariamente.

As copias deverão ser armazenadas em local seguro externo em uma NAS para evitar perda de dados. Neste local deverá haver permanentemente um conjunto completo de backup capaz de restaurar todos os dados da SPG em caso de sinistro.

Validação do Backup – Mensalmente o backup deverá ser testado pelo setor de TI, voltando-se parte ou todo o conteúdo do backup em um local previamente definido. Esta operação deverá ser acompanhada pelo gestor responsável por supervisionar a área de Ti.

Como redundância é realizado diariamente uma cópia de forma automatizada pelo Backup Azure Nuvem com programa nos servidores de aplicação ERP, Banco de dados e Arquivos. Assim como o Backup em NAS o backup Azure Nuvem deverá ser testado pelo setor de TI, voltando-se parte ou todo o conteúdo do backup em um HD previamente definido. Esta operação deverá ser acompanhada pelo gestor responsável por supervisionar a área.

14. CÓPIAS DE SEGURANÇA DE ARQUIVOS EM DESKTOPS

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de dados e outros arquivos ou documentos, desenvolvidos pelos colaboradores, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da SPG. Estes backups deverão ser realizados nas pastas de rede.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios da SPG o Setor de TI disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup da TI.

15. SEGURANÇA E INTEGRIDADE DOS DADOS

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do Setor de Ti, assim como a manutenção, alteração e atualização de equipamentos e programas.

16. PROPRIEDADE INTELECTUAL

Pertencerão exclusivamente ao colaborador a propriedade de invenção ou de modelo de utilidade quando resultar da contribuição pessoal e no uso de recursos, dados, meios, materiais, instalações ou equipamentos próprios, nos termos do art. 91 da Lei de Propriedade Industrial de n.º 9.279, de 14 de maio de 1996.

Caso o colaborador venha a desenvolver, motivado pelo seu trabalho na SPG, em sua própria residência, e com seus próprios recursos, qualquer material tangível e intangível suscetível à registro e/ou patente cujo objeto seja de interesse da SPG, o colaborador concede, desde já, a SPG o direito de preferência na aquisição do invento, pelo período de cinco anos. Neste caso, para a fixação do preço do invento será levado em conta, os recursos utilizados, o tempo e o esforço despendido e o benefício trazido, considerando sempre que o trabalho na SPG foi vetor determinante para o colaborador desenvolver o produto.

O salário percebido pelo colaborador já inclui eventuais retribuições pela sua contribuição pessoal no desenvolvimento de invenções, criações e os modelos de utilidade. O colaborador cede e transfere para a SPG todos os direitos de autor e que lhe são conexos relativos as obras que criar, durante a vigência do contrato de trabalho, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro, gratuitamente, por prazo indeterminado, em caráter total, definitivo, irrevogável e

irretratável. O colaborador desde já autoriza a SPG a utilizar, fruir e dispor da obra por quaisquer modalidades e em qualquer país, sem que lhe seja devida qualquer tipo de contraprestação, seja ela de que natureza for.

17. ACESSO A INTERNET

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na SPG. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados. O uso da Internet será monitorado pelo Setor de TI, inclusive através de "logs" (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

A definição dos colaboradores que terão permissão para uso (navegação) da Internet é atribuição da Direção da SPG, com base em recomendação do gestor de TI. Não é permitido instalar programas provenientes da Internet nos microcomputadores da SPG, sem expressa anuência do setor de TI, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais. Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros. Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De estações de rádio;
- De conteúdo pornográfico ou relacionado a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da SPG;
- Que promovam discussão pública sobre os negócios da SPG;
- Que possibilitem a distribuição de informações de nível "Confidencial".
- Que permitam a transferência (downloads) de arquivos e/ou software ilegais.

18. USO DO CORREIO ELETRÔNICO (E-MAIL)

O correio eletrônico fornecido pela SPG é um instrumento de comunicação interna e externa para a realização do negócio da SPG. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da SPG, não podem ser contrárias à legislação vigente e nem aos princípios éticos da SPG.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis e inúteis;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da SPG;
- Possam prejudicar a imagem de outras empresas;
- Sejam incoerentes com as políticas da SPG.

Para incluir um novo usuário no correio eletrônico, a respectiva Gerência deverá fazer um pedido formal ao Setor de TI, que providenciará a inclusão do referido. A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado. Em caso de congestionamento no Sistema de correio eletrônico o Setor de TI fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.

Não será permitido o uso de e-mail gratuito (liberados em alguns sites da web), nos computadores da SPG. O Setor de TI poderá, visando evitar a entrada de vírus na SPG, bloquear o recebimento de e-mails provenientes de sites gratuitos.

19. NECESSIDADE DE NOVOS SISTEMAS, APLICATIVOS E EQUIPAMENTOS

O Setor de TI é responsável pela aplicação da Política da SPG em relação à definição de compra e substituição de “software” e “hardware”. Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de TI (hardware) deverá ser discutida com o responsável pelo setor de TI. Não é permitido a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários.

20. USO DE DISPOSITIVOS MÓVEIS

Os usuários que tiverem direito ao uso de laptop ou notebook, ou qualquer outro equipamento computacional móvel, de propriedade da SPG, devem estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
- O usuário não deve alterar a configuração do equipamento recebido. Alguns cuidados que devem ser observados:

Fora do trabalho:

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi etc.
- Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível;
- Atenção ao transportar o equipamento na rua.

Em caso de sinistro

- Registre a ocorrência em uma delegacia de polícia;
- Comunique ao seu superior imediato, setor de RH e TI;
- Envie uma cópia da ocorrência para o setor de RH.

21. RESPONSABILIDADE DOS GESTORES

Os gestores são responsáveis pelas definições dos direitos de acesso de seus colaboradores aos sistemas e informações da SPG, cabendo a eles verificar se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

O Setor de TI fará auditorias periódicas do acesso dos usuários às informações, verificando:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinada rotina e/ou informação;
- Quem acessou determinada rotina e informação;
- Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;
- Que informação ou rotina determinada o usuário acessou;
- Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

22. SISTEMAS DE TELECOMUNICAÇÕES

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da SPG, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do setor de TI, de acordo com as definições da Diretoria da SPG.

23. USO DE ANTIVÍRUS

Todo arquivo em mídia proveniente de entidade externa a SPG deve ser verificado por programa antivírus. Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de TI, via rede. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

24. PENALIDADES

Todo e qualquer usuário de recursos computadorizados da SPG tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de TI. A violação desta política de segurança é qualquer ato que:

1. Exponha a organização a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.
2. Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.
3. Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental

Todo colaborador a depender do grau de violação à Política de Segurança da Informação, estará sujeito às seguintes penalidades legais:

1. Demissão por justa causa, nos termos do artigo 482 da CLT
2. Desconto equivalente em seus vencimentos, quando for o caso
3. Advertências
4. Suspensão
5. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a SPG, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes.

O colaborar também estará sujeito as sanções acima listadas nas seguintes hipóteses:

1. Violar ou deixar de utilizar as medidas técnicas e administrativas implementadas pelas SPG para proteger os dados pessoais de, mas não se limitando, acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
2. Invadir dispositivo informático da SPG ou, por meio de sua infraestrutura, de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita, respectivamente, da SPG e/ou o usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita;
3. Se o colaborador mediante fraude furtar informações e dados de qualquer natureza da SPG por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo;Se o colaborador cometer fraude com informações (i) fornecidas pela SPG ou (ii) obtidas de terceiro, por meio da infraestrutura da SPG, induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

O colaborador responde solidariamente pela integral reparação dos danos de qualquer natureza causados:

1. A SPG;
2. Pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas da SPG, se no exercício do trabalho que lhe competir ou em razão dele realizar operações com dados pessoais.

25. SISTEMA DE HELPDESK

O objetivo do ServiceDesk é prover aos técnicos de TI um ponto único de contato (**PUC**) ou single point of contact (**SPOC**), vital para uma comunicação efetiva entre os usuários e o setor de TI. A missão principal do service desk é o restabelecimento da operação normal dos serviços

dos usuários o mais rápido possível, minimizando o impacto nos negócios causados por falhas de **TI** ou melhorias de sistema e processos.

26. TRABALHO REMOTO

- O usuário deve empregar os meios necessários para não permitir que terceiros não autorizados tenham acesso aos equipamentos que utiliza em sua atividade profissional, as informações de propriedade da SPG e dados pessoais.

- O usuário se declara ciente de que o comparecimento às dependências da SPG para a realização de atividades específicas que exijam a sua presença no estabelecimento não descaracteriza o regime de teletrabalho.

- É vedado o armazenamento de dados pessoais no dispositivo utilizado no teletrabalho, salvo se autorizado, por e-mail, pelo Encarregado.

- Não é permitido o uso de rede pública não homologados pela SPG para prover a conexão à internet.

- É vedado o armazenamento de informações pessoais como, mas não se limitando, fotos, músicas, documentos no dispositivo disponibilizado pela SPG.

- O usuário se declara ciente de que o dispositivo fornecido pela SPG está sujeito a monitoramento; logo, não há expectativa de privacidade sobre o mesmo.

- Em caso de furto, roubo ou extravio do dispositivo móvel, o usuário interno deverá providenciar imediatamente comunicação às autoridades competentes, com a lavratura de Boletim de Ocorrência. O usuário deverá entregar uma cópia do B.O. para o setor de RH, que remeterá uma reprodução do referido documento para o gestor da área de TI.

- O usuário se compromete a seguir todas as instruções acima fornecidas pela SPG.

27. TRATAMENTO DO SUPORTE DA INFORMAÇÃO

- É vedado ao usuário armazenar em qualquer tipo de suporte físico as informações e dados de qualquer natureza de propriedade da **SPG** e, sem limitação, retirá-las do interior do estabelecimento e/ou de terceiros sem a autorização expressa do gestor da área a qual esteja subordinado;

- É vedado ao usuário, sem limitação, copiar, utilizar, acessar, reproduzir, transmitir, distribuir, processar, arquivar, armazenar, eliminar, modificar, comunicar, transferir, difundir, extrair as informações e dados de qualquer natureza de propriedade da SPG armazenadas em seu(s) servidor(es) e/ou de terceiros sem a autorização expressa do gestor da área a qual esteja subordinado;

- É vedado a captura de imagens da tela dos dispositivos da SPG por qualquer processo de reprodução como, mas não se limitando, fotografia, *print screen* que contenham informações de propriedade da SPG;

- O GSIRI tem o poder de vetar, revogar, cancelar o uso de dispositivos e/ou a realização de cópia de informação de um dispositivo a qualquer momento, se verificado a existência de riscos de qualquer natureza para a SPG**.**

28. CONTROLE DE ACESSOS

28.1 Política de Senhas

Cabe ao gestor de área de TI 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:

- **os usuários (logins) individuais de colaboradores:** serão de responsabilidade do próprio colaborador, que não pode ceder a quem quer que seja seu ID (login e senha), **é pessoal e intransferível**. Isso também se aplica a qualquer sistema que venha a ter acesso dentro da **SPG** para realizar as atividades sob sua responsabilidade.
- **os usuários (logins) de terceiros**: serão de responsabilidade do gestor da área contratante e deverão ser informados, por escrito, que não podem ceder a quem quer que seja seu ID (login e senha), bem como que o ID é de **pessoal e intransferível**. Isso também se aplica a qualquer sistema que venha a ter acesso dentro da **SPG** para realizar as atividades sob sua responsabilidade.

Os níveis de segurança dos direitos de acesso serão estabelecidos pelo respectivo gestor de área.

Para mantermos a rastreabilidade das informações e confidencialidade dos dados pessoais dos funcionários é de suma importância que cada colaborador tenha seu próprio usuário, seguindo o padrão de nome.sobrenome.

A senha deve ser programada para ser trocada no primeiro acesso do colaborador. Para que a troca de senha seja efetuada, deverá atender a política de senha já existente.

A troca é obrigatória e deve ser realizada a cada 90 dias, o controle é realizado pelo AD

Requisitos necessários para atender a política de senha:

-Mínimo de 8 caracteres
-Mínimo 1 caractere especial
-Mínimo 1 caractere maiúsculo
-Mínimo 1 caractere minúsculo
-Mínimo 1 numeral
- As senhas expiram a cada 3 meses
- Não é possível utilizar as últimas 4 senhas.
- A senha não deve conter informações que remetam ao usuário, por exemplo, se o usuário for joao.silva, a senha não poderá ser Joao@123.

28.2 Regras de bloqueio

A conta é bloqueada em definitivo, após 5 tentativas falhas de acesso. Caso a conta seja bloqueada, o colaborador poderá restaurar seu acesso entrando em contato com a setor de TI, preferencialmente pelo GLPI (ferramenta de chamados).

Foi definido pelo Active Directory o bloqueio de tela, esse bloqueio ocorre após 20 minutos de inatividade do Sistemas Operacional.

28.3 Acesso a rede de computadores SPG.

A SPG disponibiliza acesso a rede de internet para os colaboradores e visitantes. Às redes são segmentadas impossibilitando a comunicação entre si.

O acesso à rede coorporativa, tanto cabeada quanto WIFI é restrita à equipamentos da SPG para fins profissionais.

O acesso à rede Visitantes WIFI é restrita à visitantes ou colaboradores que necessitem acesso. A liberação do acesso à rede WIFI deverá ser solicitada para a TI, pelo Gestor do contratante ou colaborador.

28.4 Acesso às instalações

O acesso ao interior da SPG deve ser restrito aos colaboradores.

Visitantes devem ser autorizado, bem como supervisionada pelo gestor de área responsável pela sua entrada no estabelecimento da SPG.

29. CONTRATAÇÃO E MANUTENÇÃO DE EQUIPAMENTOS E SERVIÇOS

- Caberá ao gestor da área definir os requisitos do equipamento e/ou serviço que será, respectivamente, adquirido e/ou contratado, bem como de elaborar os requisitos para analisar e avaliar o fornecedor. O gestor da área poderá solicitar o apoio de outros gestores na elaboração dos requisitos do equipamento e/ou serviço e os quesitos para análise e avaliação do fornecedor;

- Em caso de acesso remoto, o acesso remoto deve ser aprovado pelo Gestor de Segurança da Informação e documentado. O acesso remoto deve durar apenas o tempo necessário para a manutenção do equipamento;

- Antes da aquisição de um software, o mesmo deve ser inspecionado pelo gestor de área de TI e validado se está adequado com as diretrizes de segurança da SPG.

30. ORGANIZAÇÃO E CUIDADOS GERAIS

- As informações de propriedade da SPG e/ou dados pessoais, contidas em suporte físico, devem ser guardados pelo usuário em uma mobília de segurança.

  Os equipamentos que não estiverem sob a supervisão do usuário, devem ser desligados ou protegidos com mecanismo de travamento automático de tela e/ou teclado controlado por senha após 20 (vinte) minutos de inatividade;

- Os documentos classificados como confidencial e interno, bem como aquele que contenham dados pessoais devem ser removidos da impressora imediatamente após impressos.

- Cabe ao usuário quando deixar seu dispositivo informático sem vigilância bloqueá-lo com o “Ctrl+alt+delete” ou “botão iniciar do Windows +l.

- É vedado o armazenamento de senhas em papeis ou documentos físicos.

31. TRANSFERÊNCIA DE INFORMAÇÃO

- Os meios de transferência da informação pela Internet, intranet, extranet, nuvem pública ou privada contratadas pela SPG, ferramentas de envio de mensagens eletrônicas como, mas não se limitando, e-mail, Whatsapp disponibilizados pela SPG devem ser utilizados estritamente para o negócio; sendo vedada a utilização para fins particulares.

- É vedado ao usuário deixar informações confidenciais, internas e dados pessoais armazenados, sem limitação, secretária eletrônicas, correio de voz, dispositivos móveis, unidades de armazenamento móvel.

32. TRATAMENTO DOS DESVIOS E EXCEÇÕES À PSI

As alterações ou exceções a Política de Segurança da Informação e Privacidade devem ser encaminhadas, por e-mail, ao setor de TI.

O setor de TI convocará o Comitê de Segurança da Informação e Respostas a Incidentes para avaliar as solicitações;

Caso a alteração ou exceção envolva dados pessoais, o gestor direto deverá ser convocado para se reunir com o CSIRI;

33. REVISÃO E ATUALIZAÇÃO:

Comitê de Segurança da Informação e Respostas a Incidentes

Periocidade: anual.

Data da última revisão: 31/08/2021

Disponível em: https://www.SPG.com.br/rh/img/clients/Politica_TI.pdf

34. DO COMPROMETIMENTO DA ALTA DIREÇÃO:

A alta direção da Organização está totalmente comprometida com a segurança da informação. Por esta razão, cumprirá fielmente todas as diretrizes previstas na Política de Segurança da Informação e Privacidade e exigirá que todos desempenhem suas responsabilidades com o mesmo rigor para proteger as informações da Organização.

_____