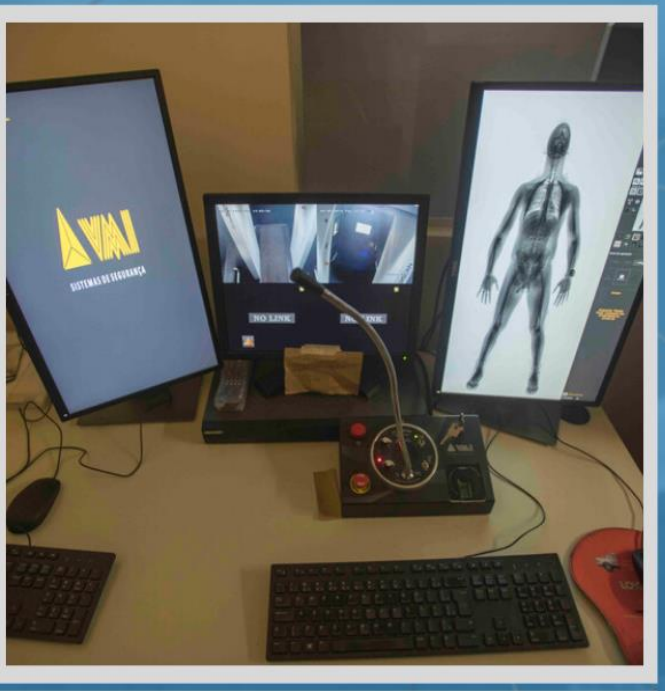
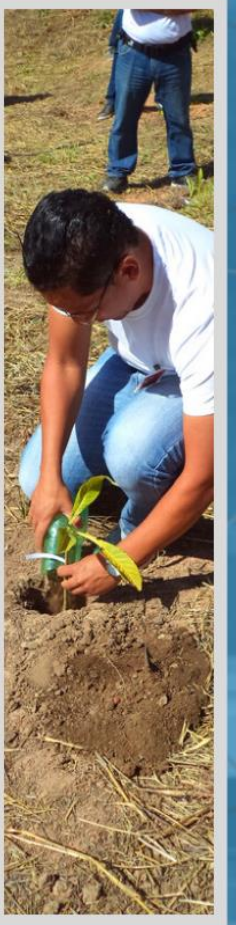
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

POLÍTICA - PL





GPA

SUMÁRIO

1. Introdução - Objetivo específico

Tem como objetivo salvaguardar e proteger a informação, bem como, orientar quanto a utilização dos recursos de informática e telefonia da Gestores Prisionais Associados S.A. (GPA), com a finalidade de proteger os colaboradores, servidores, visitantes e a empresa quanto à atuação de hackers (pirata eletrônico), contaminação lógica por 'vírus' e danificação do hardware, o que poderia comprometer a utilização dos sistemas, os serviços da rede, além de gerar problemas legais.

A segurança da informação efetiva é um trabalho em equipe envolvendo a participação, conscientização e colaboração de todos os colaboradores e/ou usuários de meios e acessos de comunicação disponibilizados pela GPA.

É de responsabilidade de cada usuário que manipula informações e/ou sistemas de informações disponibilizados, assim como conhecer esta política e conduzir suas atividades de acordo com a mesma.

2. Abrangência

Esta política se aplica a todos os funcionários, diretores, executivos, prestadores de serviços, consultores, estagiários, temporários e demais colaboradores que estejam a serviço da GPA, incluindo toda a mão- de-obra terceirizada, parcerias ou quaisquer outras formas de atuação conjunta com outras empresas.

Compreende em todos os sistemas e equipamentos de propriedade da GPA, ofertados como empréstimos/patrimônio bem como aqueles de propriedade de terceiros que lhe sejam confiados a qualquer título, ou cedidos a terceiros para execução e acesso às informações da Concessionária.

3. Definições

A Política de Segurança da Informação objetiva proteger a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios minimizando os danos e maximizando o retorno dos investimentos.

3.1 Informação

Conforme definição das normas ABNT NBR ISO/IEC 27002:2005, a informação é um ativo importante sensível para os negócios, que agrega valor para a organização e, consequentemente, necessita ser adequadamente tratada e protegida.

3.2 Vírus de computador

Não surgem do nada, são colocados em circulação através de um pequeno programa que se autocopia e/ou faz alterações em arquivos e programas, de preferência sem o seu conhecimento e/ou autorização. Suas manifestações podem se apresentar como mensagens,

alterar determinados tipos de arquivos, diminuir a performance do sistema, deletar arquivos, corromper a tabela de alocação ou mesmo apagar todo disco rígido.

3.3 Segurança

É o ato ou efeito de torne-se estável. Estado de condição de perigo e incertezas de danos e riscos eventuais. estabilidade. A segurança da informação é aqui caracterizada pela preservação da Confidencialidade, Integridade e Disponibilidade.

3.4 Confidencialidade

É a garantia de que a informação é acessível somente a pessoas com acesso autorizado, ou seja, não permitir o acesso indevido às informações, mantendo-as em sigilo.

3.6 Integridade

Estado ou característica daquilo que está inteiro, que não sofreu qualquer diminuição. É a característica ou estado daquilo que se apresenta ileso, intato, que não foi atingido ou agredido.

É essencial que a informação não seja modificada indevidamente.

3.7 Disponibilidade

Propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

3.8 Autenticidade da Informação

Propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.

3.9 Hackers

Pessoa com profundo conhecimento de informática que eventualmente os utiliza para violar sistemas ou exercer outras atividades ilegais.

Para assegurar os itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra furto, vazamento intencional ou não, fraude, espionagem, acidentes e outras ameaças.

É fundamental para a proteção e salva guarda das informações que os usuários adotem a ação de Comportamento Seguro e consistente com o objetivo de proteção das informações, devendo assumir atitudes proativas e engajadas neste aspecto.

Campanhas contínuas de conscientização de Segurança da Informação (SI) serão utilizadas para monitoramento, controle e cumprimento destas diretrizes.

3.10 Impressão digital

Captação das linhas da impressão digital por meio de um leitor biométrico que impulsiona o sistema a compará-lo com seu banco de dados.

4. Procedimento

Dar 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. 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 TI sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

5. Responsabilidades

- Cabe a todos os colaboradores -funcionários, estagiários, parceiros e prestadores de serviços, cumprir fielmente a Política de Segurança da Informação;

- Buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação;

- Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados;

- Assegurar que os recursos tecnológicos à disposição sejam utilizados apenas para as finalidades aprovadas pela GPA;

- Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual, e;

- Comunicar imediatamente a empresa quando do descumprimento ou violação desta política, por meio do canal de denúncias do programa de integridade empresarial da GPA.

5.1 Diretorias, Gerências e Coordenações

Cabe às Diretorias, Gerências e Coordenações divulgar e assegurar o cumprimento das diretrizes contidas nesta Política de Segurança da Informação, comunicando imediatamente, eventuais casos de violação ou comprometimento da segurança da informação.

Espera-se postura condizente em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

5.2 Colaboradores em geral

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à GPA e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

6. Governança de TI e Gestão da Integridade Empresarial

Cabe à Gerência de TI e à Gerência de Inteligência implementar, propor melhorias e aprimoramentos na execução desta Política, bem como, convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta Política; prover todas as informações de gestão de segurança da informação solicitadas pelos Gestores Prisionais Associados. Fica sob a responsabilidade do setor de Qualidade a fiscalização do cumprimento deste, assim como relatar os desvios encontrados.

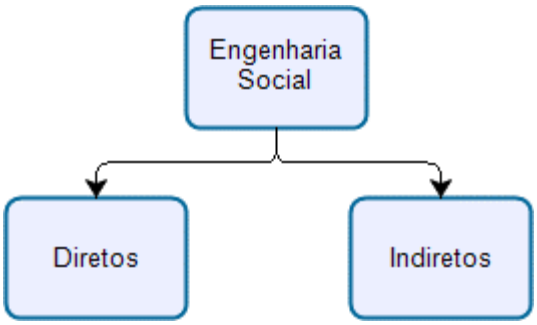
7. Propriedade intelectual

É de propriedade da GPA, todos os “designs”, fluxos, formulários, criações ou procedimentos desenvolvidos por qualquer colaborador durante o curso de seu vínculo empregatício com a GPA, sendo padronizados pelo setor de Qualidade.

8. Engenharia Social

Engenharia social é um termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações sigilosas.

A Engenharia Social manifesta-se de diversas formas, e podemos dividi-los em dois grupos:



8.1 Diretos

São aqueles caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas e até mesmo pessoalmente, considerando que em muitos casos, o engenheiro social é alguém desconhecido.

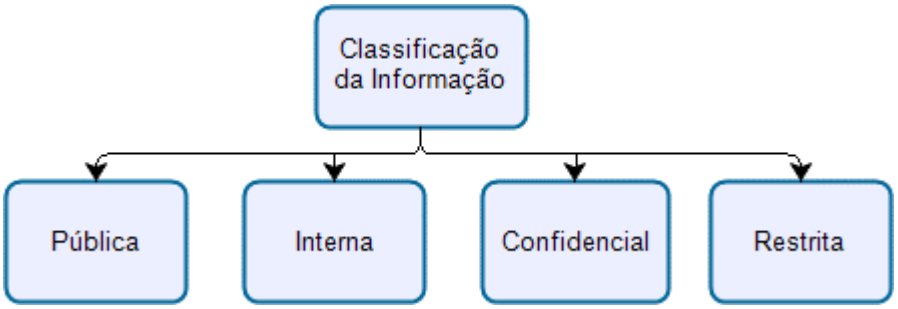
8.2 Indiretos

Caracterizam-se pela utilização de *softwares* ou ferramentas para invadir como, por exemplo, vírus, cavalos de Tróia ou através de sites e e-mails falsos para assim obter informações desejadas. Podem ser mensagens que contenham avisos de premiações milionárias em loterias, ofertas de sociedade em grandes somas de dinheiro, heranças e negócios em outros países, etc. Orienta-se que mensagens dessanatureza sejam ignoradas e o e-mail apagado

imediatamente.

9. Classificação da Informação

É de responsabilidade do Gerente/Coordenador de cada área, estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com os critérios a seguir:



9.1 Pública

É uma informação da GPA com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma ou de acordo com o interesse da empresa em dar notícia.

9.2 Interna

É uma informação da GPA sem o interesse na divulgação, onde o acesso por parte de indivíduos externosà empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os colaboradores e prestadores de serviços da GPA.

9.3 Confidencial

É uma informação crítica para os negócios da GPA. A divulgação não autorizada dessa informação podecausar impactos de ordem financeira, de imagem, operacional ou ainda, sanções administrativas, civis ecriminais à GPA. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por colaboradores, clientes e/ou fornecedores.

9.4 Restrita

É toda informação que pode ser acessada somente por usuários da GPA 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 organização.

10. Requisitos de segurança do ambiente físico

As máquinas (servidores) que armazenam os sistemas da GPA estão em área protegida, no *Data Center* localizado no ambiente da Célula-Mãe.

A entrada no *Data Center* e Salas Técnicas possui o acesso devidamente controlado por sistema de controle de acesso biométrico, sendo estes locais monitorados por câmeras e dotados de sistema de detecção de incêndio.

O *Data Center* e Salas Técnicas terão suas condições ambientais monitoradas quanto a temperatura e umidade, de forma que sejam detectadas as condições que possam afetar negativamente os recursos deprocessamento da informação.

Ambiente	Temperatura
Data Center	+/- 20 ºC
Sala técnicas	+/- 23 ºC

Todos os equipamentos localizados no *Data Center e* Salas Técnicas são alimentados por energia elétricaprovenientes de Nobreaks e Grupo Motor Gerador de forma a garantir que o processamento de dados continue mesmo se houver uma interrupção prolongada do suprimento de energia por parte da Concessionária.

A segurança de todo cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações do Complexo Penitenciário deverá ser protegido contra interceptação não autorizada ou danos.

Em todos os cabos e equipamentos, devem ser utilizadas marcações claramente identificáveis, a fim de minimizar erros de manuseio, como, por exemplo, fazer de forma acidental conexões erradas em cabos da rede.

O acesso a estas áreas por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e até mesmo colaboradores, sem acesso liberado), que necessitarem ter acesso físico ao local, sempre o farãoacompanhados de pessoas autorizadas.

11. Restrições

É vedado o acesso às dependências da GPA com quaisquer equipamentos de gravação, fotografia, vídeo,som, celulares ou outro tipo de equipamento similar, exceto aqueles que por consentimento prévio foremautorizados e mediante supervisão da área Operacional.

Respeitar áreas de acesso restrito, não executando tentativas de acesso às mesmas, ou utilizando máquinas alheias às permissões de acesso delimitadas a cada categoria de colaboradores.

12. Boas práticas de comunicação verbal dentro e fora da empresa – Código de Ética

Orienta-se para que os assuntos da empresa sejam tratados com cuidado dentro e fora do ambiente de trabalho assim como em locais públicos, ou próximos a visitantes, de forma presencial, eletrônica telefone,e-mails e mensagens.

Também, orienta-se para que seja evitado nomes e tratativas de assuntos restritos confidenciais, nestassituações, fora da empresa ou próximos a pessoas desconhecidas.

Caso seja extremamente necessária a comunicação de assuntos sigilosos em ambientes públicos, ficar atento as pessoas à sua volta que poderão usar as informações com o intuito de prejudicar a imagem da empresa.

13. Requisitos de Segurança do ambiente lógico

A GPA, 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 julgada 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.

13.1 Diretrizes Gerais

Todo acesso às informações e aos ambientes lógicos devem ser controlados, de forma a garantir acessoapenas às pessoas autorizadas.

O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registradosob a responsabilidade de cada área e em formulário, assim como suas atualizações e confirmações.

Os dados, as informações e os sistemas de informação da GPA devem ser protegidos contra ameaças eações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses ativos.

13.2 Diretrizes sobre Sistemas

Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas por usuários autorizados.

O responsável pela autorização deve ser sempre o gestor da área solicitante, o qual deve formalizar o pedido e aprovação concedida.

Cópia de segurança (Backup) deve ser testada e mantida atualizada pela área de TI para fins de recuperação em caso de desastres.

Não executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou totalde arquivos ou a indisponibilidade de serviços.

Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da GPA.

Não enviar informações confidenciais (autorizadas) para e-mails externos sem proteção. No mínimo, o arquivo deve contar com a proteção de uma senha “forte”.

13.3 Computadores e Recursos tecnológicos – Estação de trabalho

Os equipamentos disponíveis aos colaboradores são de propriedade da GPA, cabendo a cada um utiliza-lós e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

As estações de trabalho, incluindo equipamentos portáteis, e informações devem ser protegidos contra danos ou perdas, bem como o acesso, uso ou exposição indevidos.

As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do colaborador.

O acesso a estação de trabalho deverá ser encerrado no final do expediente, desligando o equipamento, respeitando o horário de expediente de trabalho. Casos em que haja necessidade de prorrogação do horário de trabalho, este pedido deverá ser efetuado antecipadamente através de preenchimento do formulário DPE-63 – Liberação _ Bloqueio de acesso – TI disponível e acessível em **G:\Politicas Gpa\Administrativo\Recursos H. e Departamento P\DPE - Formulários**, devidamente assinado pelo gestorda área solicitante e que este formulário seja anexado a um chamado no 'Portal de Chamados.

Quando se ausentar da mesa, a estação de trabalho deverá ser bloqueada com senha. Esta ação aplica-se a todos os colaboradores com estações de trabalho, incluindo equipamentos portáteis.

Informações sigilosas, corporativas ou cuja divulgação possa causar danos à GPA, só devem ser utilizadas em equipamentos com controles adequados.

Todos colaboradores, usuários da infraestrutura de TI, devem utilizar apenas softwares devidamente licenciados pela área de Suporte Técnico, nos equipamentos cedidos pela GPA.

Somente a área de Infraestrutura de TI deverá estabelecer os aspectos de controle, distribuição e instalação de softwares necessários.

Recomenda-se que todas as estações de trabalho sejam devidamente desligadas para que as atualizações programadas pela T.I se comportem conforme o esperado nos sistemas operacionais.

13.4 Dispositivos móveis

A GPA deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores, por isso, permiteque eles usem equipamentos portáteis.

Entende-se como “dispositivo móvel”, qualquer equipamento eletrônico com atribuições de mobilidade depropriedade da instituição, ou aprovado e permitido por sua Gerência de TI como: notebooks, smartphones e HD externo.

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.

A GPA reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

13.5 Utilização de equipamentos particulares / terceiros dentro da GPA

Notebooks particulares somente poderão ser trazidos para as dependências internas da GPA mediante autorização prévia da área de segurança operacional da GPA, e para acesso à rede Wi-Fi de visitantes da GPA, primeiramente deverão ser avaliados e configurados pelo responsável técnico de TI mediante abertura de chamado.

Esta avaliação de atualização de antivírus e existência de vírus será realizada pela equipe de suporte técnico da TI, mediante solicitação prévia da área visitada/contratante através de abertura de chamado epreenchimento do formulário ‘TI-03 - WiFi Visitante’, disponível no seguinte link: G:\Politicas Gpa\Administrativo\Tecnologia da Informação\Formulários.

14. Boas práticas de segurança para Impressões

Documentos enviados para impressão poderão ser retirados em qualquer ilha de impressão instalada nasunidades da GPA mediante a identificação através de usuário e senha pessoal intransferível. Osdocumentos enviados para impressoras de rede que não tenham o recurso de senha deverão ser

retirados imediatamente.

A impressão de documentos sigilosos deve ser feita sob supervisão do responsável. Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não-autorizado. Isto é, documentos esquecidos nas impressoras, ou com demora para retirada, ou até mesmo em cima da mesa, podem serlidos, copiados ou levados por outro colaborador ou por alguém de fora da empresa.

Os recursos de impressão devem ser usados exclusivamente para documentos relacionados às atividades desenvolvidas e de interesse da GPA. É vedado o uso de impressão para documentos particulares, sabendo-se que todos documentos impressos podem ser auditados.

15. A Instalação de Softwares

Qualquer software que, por necessidade do serviço, necessitar ser instalado deverá ser comunicado a área de Suporte Técnico – TI, para que o mesmo possa ser homologado pelos responsáveis de TI e só assim serem disponibilizados para o setor requerente.

A empresa respeita os direitos autorais dos softwares que usa e reconhece que deve pagar o justo valorpor eles, não recomendando o uso de programas não licenciados nos computadores da empresa. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) na GPA.

A Gerência de TI poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

16. Diretrizes quanto à utilização da Rede Corporativa

Somente usuários previamente cadastrados e autorizados possuem acesso à rede corporativa GPA. A solicitação deverá ser feita formalmente pelo gestor da área solicitante, através de formulário especifico devidamente assinado, enviado ao departamento de TI disponível na rede G:\Politicas Gpa\Administrativo\Tecnologia da Informação\Formulários.

Fica proibido a exposição, armazenamento, distribuição, edição, gravação materiais de caráter sexual através do uso dos recursos computacionais da rede corporativa.

Somente os empregados que estão devidamente autorizados a falar em nome da empresa para os meios de comunicação podem se inscrever em nome da empresa em sites de Bate-Papo (Chat Room) ou Grupos de Discussão (fóruns, newsgroups). Em caso de dúvidas, procurar a área de Comunicação da GPA ou a Diretoria.

Todos os arquivos devem ser gravados na rede GPA (G:), organizados em subpastas do respectivo setor.Os arquivos gravados no computador (local) não possuem cópias de segurança (backup) e podem ser perdidos. O espaço em disco é controlado por departamento, por isso, os usuários devem

administrar seus arquivos gravados, excluindo os arquivos desnecessários. Não é responsabilidade da área de TI a recuperação de arquivos que não respeitem a regra acima citada.

Arquivos que estiverem na rede por mais de 24 meses sem acesso, sem uma temporalidade estabelecida,serão copiados para um arquivo morto via Backup específico e excluídos após. Para ter acesso a essesarquivos, será necessário solicitar a TI através de chamado.

Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, entre outros) nos drivers derede.

Há uma autenticação adicional necessária para controlar o acesso de dispositivos móveis às redes sem fios (WiFi) disponíveis somente nas áreas administrativas das unidades, sendo necessário uma solicitação formal do gestor da área solicitante, através de formulário especifico devidamente assinado, enviado ao departamento de TI.

17. Diretrizes quanto ao uso de Mídias Removíveis e de portas USB

Não é permitida a utilização de pen drives e outros dispositivos de armazenamento, com exceção de HDsexternos quando justificado o seu uso e com prévia autorização das áreas de segurança e TI da GPA.

A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais neste caso, os pens drives merecem a atenção. Tal vulnerabilidadenão pode ser contida com *firewalls* ou com programas antivírus já que os dispositivos são acoplados aosequipamentos pelos próprios funcionários da empresa.

Para liberação das portas USB dos desktops e notebooks será necessário justificar o uso e a aprovaçãoda chefia do departamento solicitante. Para os computadores de coordenadores, gerentes e diretoria está liberação é efetuada por padrão.

Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, pois este tipo de mídia pode conter vírus esoftwares maliciosos podendo danificar e corromper dados.

De forma a evitar que informações sensíveis armazenadas em mídias removíveis sejam acessadas inadvertidamente por pessoas não autorizadas, caso ocorra a perda ou roubo do dispositivo, deve-se adotar uma chave de criptografia forte (letras maiúsculas e minúsculas, números e símbolos) através dorecurso MS Bit-Locker, a qual será utilizada como senha para liberação de acesso.

É vedado aos usuários utilizarem as mídias removíveis como meio preferencial de armazenamento de informações corporativas.

Mídias contendo informações sensíveis devem ser guardadas e destruídas de forma segura e protegida,como, por exemplo, através de incineração ou trituração, ou da remoção dos dados e formatação caso venha a ser usado para outra aplicação dentro da GPA.

18. Diretrizes quanto ao uso da Internet

A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadasà empresa.

O acesso às páginas e web sites é de responsabilidade de cada usuário ficando vedado o acesso a sitescom conteúdo impróprio e de relacionamentos.

O uso da internet para assuntos pessoais será restrito, visando não comprometer as atividades dos usuários.

É vedado qualquer tipo de download de software não autorizado, bem como, o *upload* de dados de propriedade da empresa, sem expressa autorização do gestor responsável pelo software ou pelos dados.

Os acessos à internet são monitorados através de identificação e autenticação do usuário.

Há políticas de acesso estabelecidas no *Firewall*, de acordo com o perfil de cada usuário e seu respectivo ponto de rede, de forma a garantir a segurança da informação por meio de bloqueio automático e restriçãode acesso a conteúdo não autorizado. Qualquer exceção à regra estabelecida deverá ser solicitada e justificada pelo gestor imediato à Gerência de TI.

Os colaboradores com acesso à internet não poderão efetuar o upload (envio) de arquivo, documento, imagem, ou qualquer outro meio que contenha dados pessoais sob a tutela da empresa sem o prévio conhecimento e autorização do Controlador (GPA). O compartilhamento de dados pessoais deve ser realizado de acordo com as normas, procedimentos e orientações da GPA referentes à proteção de dados pessoais.

19. Recomendações sobre o uso do Correio Eletrônico (e-mail)

É vedado o uso de sistemas webmail externo. O uso do correio eletrônico para envio e recepção de e- mail deverá ocorrer apenas através do correio eletrônico da GPA.

É proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer ou causar danos operacionais, financeiros e à imagem da empresa perante o Estado, os fornecedores e a comunidade em geral e todas aquelas que não possuem prévia autorização do gestor imediato.

Também fica vedada, a utilização do e-mail da empresa para assuntos pessoais.

É assegurado a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos decomunicação, sendo esses recursos uma ferramenta para comunicação e produtividade que deve ser usada exclusivamente para atividades corporativas, e por ser propriedade da empresa poderão ser escrutinadas e auditadas pelas áreas competentes.

Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat., exe., scr., link e com ou de quaisquer outros formatos alertados pela área de TI.

Orienta-se para não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, aviso de vírus, avisos da Microsoft, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, entre outros.

O e-mail deve ser utilizado para comunicações oficiais internas, as quais não necessitem obrigatoriamentedo meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura do documento.

A utilização do e-mail/webmail da empresa fora do horário de trabalho para posições que possuam controle de jornada deve ser aprovado pelo gestor da área.

É proibido anexar documentos ou qualquer arquivo em mensagens de correio eletrônico que contenham dados pessoais sob a tutela da GPA, exceto quando autorizado por seu gestor imediato, também é proibido o envio de dados desse mesmo tipo no corpo das mensagens.

20. Antivírus

Antivírus dos servidores e estações são atualizados automaticamente.

A varredura por vírus é feita diariamente nas estações e nos servidores, através de programas e processos automatizados definidos pelo setor de TI.

Recomenda-se que seja instalado um antivírus no dispositivo móvel, mesmo que particular, utilizado paraacesso e compartilhamento de informações corporativas, de forma a prevenir-se contra o" phishing" ("site" enganoso, utilizado como isca para acessar informações confidenciais) e o" malware" (programas maliciosos).

21. Uso de Softwares de Mensageria

A instalação e liberação de acesso aos softwares de mensageria são restritas e sua utilização deve

ser justificada e liberada pela Gerência de TI.

O uso de sistemas de mensageria é aceitável apenas quando for utilizado como ferramenta corporativa de produtividade para comunicação online, no exercício de sua função.

Sistemas de mensageria possuem histórico de riscos associados à malwares (vírus, programas maliciosos, entre outros), de forma que deve ser utilizado com zelo e cuidado.

O uso de sistemas de mensageria em redes de relacionamento pessoal é restrito no ambiente corporativo.

O grande problema de se utilizar este tipo de software é que, uma vez conectado, o computador fica altamente vulnerável. As portas de entrada/saída ficam abertas, sem qualquer restrição de leitura ou gravação. Desta forma, vírus que exploram esse tipo de vulnerabilidade não encontram empecilhos parase instalarem e iniciarem os processos danosos, não só para aquele dispositivo, mas para todos os que estiverem conectados em rede.

Exemplos de softwares de Mensageria mais populares: WhatsApp, MS Messenger, MS Skype, Google Hangouts, Telegram entre outros.

A GPA é proprietária de informações confidenciais, que devem ser compartilhadas exclusivamente através do e-mail corporativo ou da plataforma Microsoft TEAMS, meios oficiais de colaboração.

Informações que dizem respeito à empresa não podem ser compartilhadas por meio de aplicativos de mensagens ou redes sociais.

Informações da GPA, de cunho profissional e confidencial, não devem se misturar com assuntos da vidapessoal, principalmente quando se utiliza o mesmo aplicativo e dispositivo móvel para acesso.

A utilização de aplicativos corporativos de mensagens deve se restringir ao horário de trabalho. Qualquer exceção a esta regra, deverá ser aprovada previamente pelo gestor da área, bem como pelo colaborador que possua controle de jornada, através de um termo de consentimento controlado pela área de RH.

22. Controle de Acesso a VPN

O acesso remoto via VPN é restrito apenas aos usuários que o solicite mediante autorização e justificativaprévia do gestor da área solicitante, sendo este acesso de uso exclusivo para as finalidades relacionadas à sua função, às suas atividades e que seja de interesse da GPA, devendo abster-se de usar a funcionalidade para quaisquer outras atividades.

O acesso remoto via VPN será concedido, mediante justificativa e autorização, apenas para equipamentos ativos de propriedade da GPA.

É vetado aos usuários do serviço compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros funcionários outerceiros.

O acesso VPN implica em riscos para a rede corporativa, uma vez que com ele é possível acessar à mesma, de forma privilegiada, a partir de qualquer ponto da internet, como se o usuário estivesse fisicamente nas instalações da GPA.

Nunca deixar sessões VPN abertas, cada vez que o usuário deixar o seu equipamento conectado via VPN, deve executar logoff/ logout ou bloquear seu equipamento.

Manter-se conectado à rede via acesso VPN apenas pelo tempo necessário à execução da tarefa que requereu o uso do serviço.

23. Controle de Acesso Lógico (Baseado em Senhas)

Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal.

Utilizar senha de qualidade “forte”, com pelo menos (7) sete caracteres contendo no mínimo (1) um número, (1ª) uma letra (maiúscula ou minúscula) e no mínimo (1) um caractere especial (símbolos), e nãodeve conter nome, sobrenome, ou senha usada anteriormente, uma vez que é necessária uma nova senha ou alterá-la a cada 3 (três) meses.

Utilizar um método próprio para lembrar-se da senha, de modo que ela não precise ser anotada em nenhum local, em hipótese alguma.

Não incluir senhas em processos automáticos de acesso ao sistema por exemplo, armazenadas em macros ou teclas de função.

A distribuição de senhas aos usuários (inicial ou não) deve ser feita de forma segura. A senha

concedidainicialmente, deve ser trocada pelo usuário em seu primeiro acesso.

A troca de uma senha bloqueada só deve ser liberada por solicitação do próprio usuário ao departamentode TI, mediante confirmação de alguns dados pessoais.

Foi estabelecido um procedimento formal de registro e cancelamento de usuário, através de formulários específicos devidamente assinados pelo gestor da área solicitante, de forma a garantir e revogar acessosem todos os sistemas de informação e serviços. Cabe ao gestor de cada área solicitante estabelecer o perfil de acesso típico que será concedido ao usuário, baseando-se nos requisitos da área, na função exercida, no direito e privilégios de acessos.

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

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

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores. Todos os dispositivos de identificação utilizados na GPA, 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.

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

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outraspessoas em nenhuma hipótese

24. Controle de Acesso Biométrico - Leitura das digitais

A confiança depositada na biometria está baseada na segurança que a mesma entrega. O sistema biométrico se baseia nas características únicas de certas partes do corpo humano.

Na GPA atualmente utilizamos as digitais dos dedos, onde o sistema captura a imagem da impressão digital dodedo através de um leitor óptico. Dessa informação, cria-se um banco de dados com digitais previamente gravadas, gerando assim um sistema que garante segurança no controle de acesso de colaboradores e visitantes.

25. Tratamento de incidentes de segurança da informação

Identificar e classificar o tipo de incidente: vírus, invasão, informação sigilosa, divulgação não

autorizada,entre outros. Existem duas categorias para este tipo de incidente: invasão tecnológica ou informação passada.

25.1 Informação propriamente dita

Cabe abertura de processo de oitiva, conduzida pelo setor de inteligência. Invasão tecnológica.

25.2 Equipamento da rede

Consiste na comunicação imediata através da abertura de chamado, análise e mensuração do impacto e propor uma resposta para conter e eliminar o incidente.
Formatar ou restaurar os equipamentos afetados, visando a recuperação dos serviços impactados.

26. Violações da política de segurança da informação e sanções

As violações ao conteúdo desta política serão objeto de comunicações e respectivas avaliações quanto à sua natureza, amplitude e gravidade, estando sujeitas as sanções trabalhistas, além de responsabilidades cíveis e criminais cabíveis.

As infrações às determinações constantes desta política, dependendo de sua extensão, poderão ser objeto de procedimento apuratório específico, levados a efeito pelo Comitê de Ética, auxiliado pela Gerência de TI.

O Código de Conduta e Ética e o Regimento Interno da Empresa deverão ser observados integralmente, especialmente por ocasião de situações de tratamento das informações.

O funcionário infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato, ao Comitê de Ética e à Diretoria.

27. Canal de ética

E-mail: etica@gpamg.com.br

28. Vigência e Validade

A presente política passa a vigorar a partir da data de sua validação e publicação, sendo válida por tempoindeterminado, devendo ser revisada anualmente ou sempre que necessário para adequação e melhoriado processo.

29. Lista de Siglas e conceitos

TI: Tecnologia da Informação.
Software: É a parte lógica, o conjunto de instruções e dados processados nos servidores e

computadores.Toda interação dos usuários de computadores é realizada através de softwares.

Backup: É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restauradoem caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Mídias Removíveis: Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Pen Drive, cartão de memória entre outros.

USB: É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.

VPN (Virtual Private Network): Modalidade de acesso à rede corporativa, que possibilita a conectividade,via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna.

Softwares de Mensageria: São programas que permitem a usuários se comunicarem remotamente (à distância), através de conexão com a Internet. Por meio destes programas, é possível enviar mensagensde texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessõesde conversação com áudio e/ou com vídeo, em tempo real.

Firewall: É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

HISTÓRICO DAS ALTERAÇÕES				
POLITICA DE SEGURANÇA DE INFORMAÇÃO – PSI				
Revisão	Data	Descrição da alteração	Elaborado por:	Controle da Qualidade
00	22/09/2020	Elaboração e publicação	Sérgio Pergolaro	Thamires Pereira / Cristiane
01	04/11/2020	Alteração no item 13.3	Sérgio Pergolaro	Thamires Pereira / Cristiane
02	11/08/2022	Alteração nos itens 3.6, 18, 19, 26 e 27	Sérgio Pergolaro	Cristhiano Gurgel / Ana Carolina
02	11/08/2022	Inclusão do item 3.7 e 24	Sérgio Pergolaro	Cristhiano Gurgel / Ana Carolina