GOVERNANÇA DA INFORMAÇÃO

PSI – Política de Segurança da Informação

Índice

OBJETIVOS 4
APLICAÇÕES DA PSI 4
PRINCÍPIOS DA PSI 4
REQUISITOS DA PSI 5
DAS RESPONSABILIDADES ESPECÍFICAS 6
1 - Dos Profissionais em Geral (Colaborador) 6
2 - Dos Profissionais em Regime de Exceção (Temporários, chamados de “Freelas”) 6
3 - Dos Gestores de Pessoas e/ou Processos 6
4 – Os donos das Informações 6
5 - Dos Custodiantes da Informação 6
5.1 - Da Área de Tecnologia da Informação 6
5.2 - Da Área de Segurança da Informação (A ser criada) 8
5.3 - Do Comitê de Segurança da Informação – CSI - (A ser desmembrado do Comitê de Automação ou Ser Criado)
8
6 - DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE 9
CORREIO ELETRÔNICO 10
INTERNET 11
IDENTIFICAÇÃO 12
COMPUTADORES E RECURSOS TECNOLÓGICOS 13
DISPOSITIVOS MÓVEIS 15
DATACENTER 16
BACKUP 17
PROPRIEDADE INTELECTUAL E CONFIDENCIALIDADE 18
DAS DISPOSIÇÕES FINAIS 18

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas das empresas que fazem parte do **Grupo Dreamers**, sendo esse documento referente ao GRUPO DREAMERS**,** para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país. Com a intenção de aumentar a segurança da infraestrutura tecnológica direcionada ao uso corporativo, foi desenvolvida paralelamente uma Norma de Segurança da Informação, visando a orientação de nossos usuários, clientes e fornecedores para a utilização dos ativos de tecnologia da informação disponibilizados.

A informação é um dos principais patrimônios do mundo dos negócios. Um fluxo de informação de qualidade é capaz de decidir o sucesso de um empreendimento. Mas esse poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças internas e externas. Assim, quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos ao **GRUPO DREAMERS** e prejudicar nosso crescimento e nossa vantagem competitiva.

Atentos a isso, publicamos a Política de Segurança da Informação (“PSI”), tendo como finalidade fundamental construir o alicerce de proteção aos ativos de informação de propriedade do **GRUPO DREAMERS**.

Este documento encontra-se disponível na intranet do Grupo, no endereçohttps://artplan.sharepoint.com/sites/comitedeprivacidadedadospessoais-lgpd/Documentos%20Compartilhados/Forms/AllItems.aspx?id=%2Fsites%2Fcomitedeprivacidadedadospessoais%2Dlgpd%2FDocumentos%20Compartilhados%2FPoliticas%2FA%2DLAB&viewid=570b964b%2D73fd%2D4e07%2D8612%2D400e1b9f05f6

OBJETIVOS

Estabelecer diretrizes que permitam aos Profissionais e prestadores de serviços do **GRUPO DREAMERS** seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal das empresas do Grupo e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para o seu atendimento.
Preservar as informações do GRUPO DREAMERS quanto à:

Integridade: garantia de que a informação seja mantida no seu estado original, visando protegê-la, na guarda outransmissão, contra alterações indevidas, intencionais ou acidentais.
Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

TODA INFORMAÇÃO GERADA NO GRUPO É CONFIDENCIAL

APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os Profissionais e prestadores de serviços e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência de que os ambientes, sistemas, computadores e redes de cada empresa do Grupo poderão ser monitoradose gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada Profissional ou prestador de serviços se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionados, buscando orientação dos seus Gerentes / Gestores responsáveis por estes assuntos, Comitê de Privacidade Local, ou representado pelo DPO, Data Protection Office nomeado, sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Tecnologias, marcas, metodologias e quaisquer informações relativas à propriedade intelectual que pertençam ao **GRUPO DREAMERS** não devem ser utilizadas para fins particulares nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Profissional em seu ambiente de trabalho.

PRINCÍPIOS DA PSI

Toda informação produzida ou recebida como resultado da atividade profissional contratada pelo **GRUPO DREAMERS** pertence à referida organização. As exceções devem ser explícitas e formalizadas em contrato escrito entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos Profissionais e prestadores de serviços para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços e sigam as boas práticas da Política de Traga o seu Dispositivo. (Política_de_traga_seu_próprio_dispositivo_BYOD_PT).

O **GRUPO DREAMERS**, por meio da Gerência TI, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

REQUISITOS DA PSI

Para a uniformidade da informação, a PSI será comunicada a todos os Profissionais e prestadores de serviços do **GRUPO DREAMERS**, a fim de que a política seja cumprida dentro e fora da organização.

Haverá um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designadoComitê de Segurança da Informação e ou comitê de privacidade a ser divulgado.

Tanto a PSI quanto as normas serão revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive a sua revisão antecipada, conforme análise e decisão do Comitê de Segurança. Constará em todos os contratos do **GRUPO DREAMERS** o anexo de Acordo de Confidencialidade, Cláusula de Confidencialidade ou Política de Privacidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos Profissionais ou prestadores de serviços. Todos os Profissionais devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Um Termo de Conhecimento da PSI será assinado por cada Profissional.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Gerência TI e, caso julgue necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação / Comitê de Privacidade para análise.

Um plano de contingência e a continuidade dos principais sistemas e serviços serão implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e

disponibilidade dos ativosde informação.

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

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

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

O **GRUPO DREAMERS** exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Profissionais, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta PSI será implementada no **GRUPO DREAMERS** por meio de procedimentos específicos, obrigatórios para todos os Profissionais, independentemente do nível hierárquico ou da função no Grupo, bem como de contratação via vínculo empregatício ou prestação de serviço.

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

DAS RESPONSABILIDADES ESPECÍFICAS

1 - Dos Profissionais em Geral (Colaborador)

Entende-se por Profissional toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora do **GRUPO DREAMERS**.

Será de inteira responsabilidade de cada Profissional todo prejuízo ou dano, que sofrer ou causar ao GRUPO DREAMERS e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

2 - Dos Profissionais em Regime de Exceção (Temporários, chamados de “Freelas”)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação.
A concessão poderá ser revogada a qualquer tempo por livre discricionariedade do **GRUPO DREAMERS** ou automaticamente se o Profissional que o recebeu não estiver cumprindo as condições definidas no aceite.

3 - Dos Gestores de Pessoas e/ou Processos

O departamento de Recursos Humanos exigirá dos Profissionais e prestadores de serviços no momento da contratação a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas na presente PSI, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informação do **GRUPO DREAMERS**.

Antes de conceder acesso às informações da instituição, o departamento de Recursos Humanos deverá exigir a assinatura do Acordo de Confidencialidade dos Profissionais casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostascomerciais.

O Gestor responsável de cada departamento utilizará tais normas, processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI, bem como será o responsável por cumprir tais normas perante sua equipe.

4 – Os donos das Informações

Todas as informações geradas dentro das empresas do Grupo são CONFIDENCIAIS, e devem ser tratadas como tal. Quem gera a informação é 100% responsável por sua segurança, manuseio, backup e devem estar de acordo com os processos dos Custodiantes indicados. OS DONOS DAS INFORMAÇÕES GERADAS DENTRO DO GRUPO É O GRUPO DREAMERS.

5 - Dos Custodiantes da Informação

5.1 - Da Área de Tecnologia da Informação

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais. Acordar com a empresa terceirizada o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.
Configurar equipamentos, ferramentas e sistemas concedidos aos Profissionais com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI, pelas Normas de Segurança da Informação complementares.

Os administradores e operadores dos sistemas computacionais podem, pela característica dos seus

privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for estritamente necessário para a execução de atividades operacionais sob a sua responsabilidade, como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

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

Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

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

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos erelevantes para o **GRUPO DREAMERS.**

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

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

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

Planejar, implantar, fornece e monitorar a capacidade de armazenagem, processamento e transmissão necessária para garantir a segurança requerida pelas áreas de negócio.

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 funcionários serão de responsabilidade do próprio colaborador.
- Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação das empresas do Grupo contra código malicioso e

garantir que todos os novos ativos só entrem para o ambiente de produção após estar livres de código malicioso e/ou indesejado.

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

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo oseu cumprimento dentro do Grupo.

Realizar auditorias periódicas semestrais de configurações técnicas e análise de riscos, normalmente chamada de PENTEST ou qualquer auditoria semelhante de empresas especializadas nesse tipo de trabalho.

Responsabilizar-se pelo uso, pelo manuseio, pela guarda de assinatura e pelos certificados digitais usados pelos servidores e softwares da Área de Tecnologia. Os certificados usados pelas áreas de negócios, devem ter as mesmas garantias de segurança dessa PSI para os mesmos, sendo essas responsabilidades de cada gestor em suaárea específica.

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

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

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

- Uso da capacidade instalada da rede e dos equipamentos;
- Tempo de resposta no acesso à internet e aos sistemas críticos do **GRUPO DREAMERS**;
- Períodos de indisponibilidade no acesso à internet e aos sistemas críticos do **GRUPO DREAMERS;**
- Incidentes de segurança (vírus, trojans, furtos, acessos indevidos e assim por diante);
- Atividade de todos os Profissionais durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

5.2 - Da Área de Segurança da Informação (A ser criada)

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

Propor e apoiar iniciativas para a segurança dos ativos de informação do **GRUPO DREAMERS**.

Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Comitê deSegurança da Informação ou Comitê de Privacidade.

Promover a conscientização dos Profissionais em relação à relevância da segurança da informação para o negócio do **GRUPO DREAMERS**, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ouserviços.

Analisar fundamentada e criticamente incidentes em conjunto ao Comitê de Segurança da Informação.

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

Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema queafetem ou tenham potencial para afetar ao **GRUPO DREAMERS.**

Buscar alinhamento com as diretrizes corporativas da instituição.

5.3 - Do Comitê de Segurança da Informação – CSI - (A ser desmembrado do Comitê de Automação ou Ser Criado)

Deve ser formalmente constituído por Profissionais, com nível hierárquico mínimo gerencial**,** nomeados paraparticipar do grupo pelo período de um ano.

A composição mínima deve incluir um Profissional de cada uma das áreas: Financeira, Administrativa, Tecnologiada Informação, Jurídico/Compliance e Recursos Humanos.

Deverá o **CSI** se reunir formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para o **GRUPO DREAMERS.**

O **CSI** poderá utilizar especialistas, internos ou externos, para apoiar nos assuntos que exijam conhecimentotécnico específico.

Cabe ao **CSI**:

ɾ Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
ɾ Propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;
ɾ Avaliar os incidentes de segurança e propor ações corretivas;
ɾ Definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informaçãocomplementares.

6 - DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas neste PSI, ao **GRUPO DREAMERS** poderá:

ɾ Implantar sistemas de monitoramento em estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
ɾ Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;
ɾ Realizar, a qualquer tempo, inspeção física e lógica nas máquinas de sua propriedade, bem como remover ou darqualquer acesso.
ɾ Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

CORREIO ELETRÔNICO

O objetivo desta norma é informar aos Profissionais do **GRUPO DREAMERS** quais são as atividades permitidas e proibidas no uso do correio eletrônico corporativo.

O uso do correio eletrônico do **GRUPO DREAMERS** é para fins corporativos e relacionados às atividades do Profissional usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique ao **GRUPO DREAMERS** e não cause impacto relevante no tráfego da rede.

Acrescentamos que é proibido aos Profissionais o uso do correio eletrônico do **GRUPO DREAMERS** para:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas ao uso legítimo da instituição ou que descumpram Lei Geral de Proteção de Dados Pessoais;
- Enviar mensagem por correio eletrônico pelo endereço do seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne o seu remetente e/ou ao **GRUPO DREAMERS** ou as suas unidades vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades do **GRUPO DREAMERS** estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que:
  - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do GRUPO DREAMERS;
  - contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
  - contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf)ou qualquer outra extensão que represente um risco à segurança;
  - vise obter acesso não autorizado a outro computador, servidor ou rede;
  - vise interromper um serviço, servidor ou rede de computadores por meio de qualquer método ilícito ounão autorizado;
  - vise burlar qualquer sistema de segurança.
  - vise vigiar secretamente ou assediar outro usuário.
  - vise acessar informações confidenciais sem explícita autorização do proprietário.
  - vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
  - inclua imagens criptografadas ou de qualquer forma mascaradas;
  - contenha anexo(s) superior(es) a 35 MB para envio (interno e internet) e 35 MB para recebimento(internet);
  - tenha conteúdo considerado impróprio, obsceno ou ilegal;
  - seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico,entre outros;
  - contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras

    situações protegidas.
  - tenha fins políticos locais ou do País (propaganda política);
  - inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.
  - As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:
    - Nome do Profissional

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

INTERNET

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

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o **GRUPO DREAMERS**, em total conformidade legal, reserva-se o direito de monitorar e registrartodos os acessos a ela.

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

O **GRUPO DREAMERS**, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer Profissional, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao Profissional 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.

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

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

Somente os Profissionais que estão devidamente autorizados a falar em nome do **GRUPO DREAMERS** para

os meios de comunicação poderão se manifestar, seja por e-mail, entrevista on-line, podcast, documento físico, entre outros.

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

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

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela Gerência de TI e o colaborador será penalizado de acordo com as cláusulas contratuais existentes.

Os Profissionais não poderão em hipótese nenhuma utilizar os recursos do **GRUPO DREAMERS** para fazer o download ou a distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

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

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Profissionais com acesso à internet não poderão efetuar upload (subida) de nenhum software licenciado do **GRUPO DREAMERS** ou de dados da sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os Profissionais não poderão utilizar os recursos do **GRUPO DREAMERS** para deliberadamente propagar nenhum tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

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

Não é permitido acesso a sites que visem mascarar navegações potencialmente ofensivas a PSI do Grupo e a constituição federal.

Com o crescimento da Nuvem, e aplicações CLOUD, NÃO coloquem informações do GRUPO em nuvens que não seja liberada ou possuam controle pelo GRUPO. Por exemplo, uso de WETRANSFER gratuito, onde que oWetransfer irá ter acesso a todas a nossas informações, como informações de nossos clientes. Por favor, usem o nosso Onedrive. Qualquer dúvida sobre o uso de ferramentas em nuvem, fale com o comitê de segurança ou departamento de TI.

IDENTIFICAÇÃO

Os dispositivos de identificação e as senhas protegem a identidade do Profissional usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o **GRUPO DREAMERS** e/ou terceiros.

O uso dos dispositivos e/ou das senhas de identificação de outra pessoa constitui crime tipificado no Código Penal 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 Profissionais.

Todos os dispositivos de identificação utilizados no **GRUPO DREAMERS**, como o número de registro do Profissional,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 outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um Profissional, a responsabilidade perante o **GRUPO DREAMERS** e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for

identificado conhecimentoou solicitação do gestor de uso compartilhado, ele deverá ser responsabilizado. É proibido o compartilhamento de login para funções de administração de sistemas.

O Departamento de Recursos Humanos do **GRUPO DREAMERS** é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos Profissionais.

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

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

É de responsabilidade de cada usuário a memorização da sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados. E é obrigatório o uso de senha complexa em todos os sistemas.

É política do **GRUPO DREAMERS** solicitar a troca de senha a cada 60 dias das senhas utilizadas pelos seus usuários.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras e devem ser do tipo complexa, contendo pelo menos 8 (oito caracteres), sendo esses umacombinação de: Caracteres Maiúsculos e Minúsculos, Números e caracteres especiais.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha seencerrado, bem como aos usuários de testes e outras situações similares.

Caso o Profissional esqueça a sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente àárea técnica responsável para cadastrar uma nova.

COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos Profissionais são de propriedade do **GRUPO DREAMERS**, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis. Fica proibido o uso de computadores pessoais para prestar serviços relacionados ao **GRUPO DREAMERS** de qualquer natureza, dentro ou fora do Grupo.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Gerência de TI do **GRUPO DREAMERS**, ou de quem este determinar.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação e, depois da sua disponibilização, pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no helpdesk.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio do GRUPO DREAMERS (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para os drives de rede (Nuvem), pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos Profissionais da instituição deverão ser salvos em drives de rede (Workspace – Onedrive – Nuvem). Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário. Utilize o Onedrive pessoal para tal processo. Siga as orientações da Gerência de TI e mantenha seu equipamento sincronizado com o seu Onedrive.

Os Profissionais do **GRUPO DREAMERS** e/ou detentores de contas privilegiadas não devem executar

nenhum tipo decomando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Gerência de TI.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

ᵞ Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de Profissionais não autorizados. Tais senhas serão definidas pela Gerência de TI, que terá acesso a elas para manutenção dos equipamentos.
ᵞ Os Profissionais devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado a seu computador.
ᵞ É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Gerência de TI ou por terceiros devidamente contratados para o serviço.
ᵞ É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.
ᵞ O Profissional deverá manter a configuração do equipamento disponibilizado pelo **GRUPO DREAMERS**, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.
ᵞ Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os computadores quando não estiverem sendo utilizados.
ᵞ Todos os recursos tecnológicos adquiridos pelo **GRUPO DREAMERS** devem ter imediatamente suas senhas- padrões (default) alteradas.
ᵞ Os equipamentos deverão manter preservados, de modo seguro, e com registros de eventos, constando identificação dos Profissionais, datas e horários de acesso. Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos do **GRUPO DREAMERS para:**

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário.
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores depacotes (sniffers).
- Interromper um serviço, servidor ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular.
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no País, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

- Colocar qualquer tipo de adesivo, riscar, escrever nos equipamentos.

DISPOSITIVOS MÓVEIS

O **GRUPO DREAMERS** deseja facilitar a mobilidade e o fluxo de informação entre alguns dos seus Profissionais. Por isso permite que eles usem equipamentos portáteis.

Quando se descreve “dispositivo móvel”, entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição ou aprovado e permitido pela sua Gerência de TI, como: notebooks, smartphones, Drives de HD Externos e pen drives.

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

O **GRUPO DREAMERS**, na qualidade de proprietária dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O Profissional, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo nenhum, direta ou indiretamente, em proveito próprio ou de terceiros, nenhuma informação, confidencial ou não, que tenhaou venha a ter conhecimento em razão das suas funções no **GRUPO DREAMERS**, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo Profissional deverá realizar periodicamente cópia de segurança (backup) dos dados do seu dispositivo móvel. Deverá, também, manter os seus backups separados do seu dispositivo móvel, ou seja, não os carregar juntos. Utilize o Onedrive pessoal para tal processo. Siga as orientações da Gerência de TI e mantenha seu equipamento sincronizado com o seu Onedrive.

O suporte técnico aos dispositivos móveis de propriedade do **GRUPO DREAMERS** e aos seus usuários deverá seguiro mesmo fluxo de suporte contratado pela instituição.

Todo Profissional deverá utilizar senhas de bloqueio automático para o seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, o auxílio ou a presença de um técnico da Gerência de TI.

O Profissional deverá se responsabilizar em não manter ou utilizar nenhum programa e/ou aplicativo que nãotenha sido instalado ou autorizado por um analista da Gerência de TI do **GRUPO DREAMERS**.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

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

É responsabilidade do Profissional, no caso de furto ou roubo de um dispositivo móvel fornecido pelo **GRUPO DREAMERS**, notificar imediatamente ao seu gestor direto e a Gerência de TI.

Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O Profissional deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos osriscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao **GRUPO DREAMERS** e/ou a terceiros.

DATACENTER

O acesso ao Datacenter somente deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético, entre outros.

Todo acesso ao Datacenter, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio.

Todo acesso ao Datacenter será registrado por câmeras de vídeo devidamente posicionadas na entrada do Datacenter e dentro da Sala dos Servidores.

Deverá ser executada semanalmente uma auditoria nos acessos ao Datacenter pelo Relatório do Sistema de Registro.

O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do Gerente responsável, de acordo com o Procedimento de Controle de Contas Administrativas.

A lista de funções com direito de acesso ao Datacenter deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Datacenter, e salva no diretório de rede.

Nas localidades em que não existam Profissionais da área de tecnologia da informação, pessoas de outros departamentos deverão ser cadastradas no sistema de acesso para que possam exercer as atividades

operacionais dentro do Datacenter, como: troca de fitas de backup, suporte em eventuais problemas, e assim por diante.

O acesso ao Datacenter, por chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial, ou quando o sistema de autenticação forte não estiver funcionando.

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

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

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

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

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

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

BACKUP

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

Os Profissionais responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

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

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

O tempo de vida e de uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

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

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

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

As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de sala-cofre, distante no mínimo 10 quilômetros do Datacenter.

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

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

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

Quaisquer atrasos na execução de backup ou Restore deverão ser justificados formalmente pelos

responsáveis,nos termos do Procedimento de Controle de Mídias de Backup.

Testes de restauração (Restore) de backup devem ser executados pelos seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

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

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

PROPRIEDADE INTELECTUAL E CONFIDENCIALIDADE

Tecnologias, marcas, metodologias e quaisquer informações relativas à propriedade intelectual que pertençam ao **GRUPO DREAMERS** não devem ser utilizadas, sob qualquer hipótese ou pretexto, para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Profissional no seu ambientede trabalho.

As informações e os sistemas de informação e diretórios de rede são classificados como estritamente confidenciais. As informações confidenciais necessitam de sigilo absoluto e devem ser protegidas por todos os Profissionais com acesso a essas informações. Cabem a esses Profissionais todos os esforços necessários.

Falhas no sigilo da informação, integridade ou disponibilidade desse tipo de informação trazem grandes prejuízos ao **GRUPO DREAMERS**, expressos em perdas financeiras diretas, perdas de competitividade e produtividade ou da sua imagem, podendo levar à extinção de jobs ou prejuízos graves ao crescimento do Grupo.

São exemplos de informações confidenciais: – Informações de clientes; – Informações sobre nossos serviços que revelem vantagens competitivas ao **GRUPO DREAMERS** frente ao mercado; – Toda e qualquer informação de propriedade do **GRUPO DREAMERS**; Todo o material estratégico do **GRUPO DREAMERS** (material impresso, armazenado em sistemas, em mensagens eletrônicas); – Todos os tipos de senhas a sistemas, redes e estações de trabalho.

Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos,

eletrônicos ou não. Ao usar uma impressora coletiva, recolha o documento impresso imediatamente.

Não discutir ou comentar assuntos confidenciais do **GRUPO DREAMERS** em locais públicos ou por meio de mensagens de texto, salvo no caso de uso de telefones corporativos.

DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do **GRUPO DREAMERS**. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

Canal de Denúncia:

E-mail: comitedeprivacidade@grupodreamers.com.br