Política de segurança da informação

1. **OBJETIVO**

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e audibilidade das informações necessárias para a realização dos negócios da **EGGS SOLUÇÕES IMOBILIÁRIAS/BR 153 Loteamento Empresaria**.

2. **ABRANGÊNCIA**

Aplica-se a todos os administradores, funcionários, estagiários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento, ou com acesso a informações que pertençam a **EGGS SOLUÇÕES** ou a **SEUS CLIENTES**.

Todo e qualquer usuário de recursos computacionais da empresa tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

3. **CONCEITOS**

A segurança da informação é aqui caracterizada pela preservação dos seguintes conceitos:

- **Confidencialidade**: Garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário;

- **Disponibilidade**: Garante que a informação esteja disponível para as pessoas autorizadas sempre que se faça necessário;
- **Integridade**: Garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

4. DEFINIÇÕES

Informação: resultado do processamento e organização de dados (eletrônicos ou físicos) ou registros de um sistema.

Ativos de Informação: conjunto de informações, armazenado de modo que possa ser identificado e reconhecido como valioso para a empresa.

Sistemas de informação: de maneira geral, são sistemas computacionais utilizados pela empresa para suportar suas operações.

Segregação de funções: consiste na separação entre as funções de autorização, aprovação de operações, execução, controle e contabilização, de tal maneira que nenhum funcionário, estagiário ou prestador de serviço detenha poderes e atribuições em desacordo com este princípio.

Grupo Gestor da Segurança da Informação: grupo composto por administradores da **EGGS SOLUÇÕES IMOBILIÁRIAS/BR 153 Loteamento Empresaria**.

com o objetivo de avaliar a estratégia e diretrizes de segurança da informação seguidas pela empresa.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação produzida no desenvolvimento das atividades da empresa deve ser classificada de acordo com os níveis de confidencialidade abaixo:

Pública: É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral. **Por exemplo:** informações disponíveis na página da Internet da **EGGS SOLUÇÕES IMOBILIÁRIAS/BR 153 Loteamento Empresaria**.

1. ou nas redes sociais da empresa.
2. **Interna:** É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.
3. **Confidencial:** É toda informação que pode ser acessada por usuários da organização e por parceiros da organização especificamente autorizados. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.
4. **Restrita:** É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome, e-mail e 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.

6. **RESPONSABILIDADES**

De forma geral, cabe a todos os administradores, funcionários, estagiários e prestadores de serviços:

Cumprir fielmente a Política de Segurança da Informação da **EGGS SOLUÇÕES IMOBILIÁRIAS/BR 153 Loteamento Empresaria**.

- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela **EGGS SOLUÇÕES**;

Assegurar que os recursos tecnológicos, as informações e sistemas à sua disposição sejam utilizados apenas para as finalidades aprovadas pela **EGGS SOLUÇÕES IMOBILIÁRIAS/BR 153 Loteamento Empresaria**.

- ;
- Cumprir as leis e as normas que regulamentam a propriedade intelectual;
- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais etc.), incluindo a emissão de comentários e opiniões em blogs e redes sociais;
- Não compartilhar informações confidenciais de qualquer tipo;
- Comunicar imediatamente à área de Gestão de Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.

É dever de todos dentro da EGGS SOLUÇÕES IMOBILIÁRIAS/BR 153 Loteamento Empresaria.

:

Considerar a informação como sendo um ativo da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a EGGS SOLUÇÕES e deve sempre ser tratada profissionalmente.

É de responsabilidade do Gerente/Supervisor de cada área classificar a informação (relatórios, documentos, modelos, procedimentos, planilhas) gerada por sua área de acordo com o nível de confidencialidade estabelecido neste documento.

São boas práticas:

- Bloquear o acesso ao computador sempre que sair da sua mesa de trabalho, mesmo que por alguns minutos;
- Manter mesas organizadas e documentos com informações confidenciais trancados, quando não os estiver utilizando.

7. Grupo Gestor da Segurança da Informação da EGGS SOLUÇÕES

Missão

Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

Equipe

Marco Pollo de Herval e Henrique Marcatto Gomes

8. DIRETRIZES GERAIS

1. DADOS PESSOAIS DE FUNCIONÁRIOS

A EGGS SOLUÇÕES se compromete em não acumular ou manter intencionalmente dados pessoais de funcionários além daqueles relevantes na condução do seu negócio. Todos os dados pessoais de funcionários serão considerados confidenciais.

Os dados pessoais de funcionários sob a responsabilidade da EGGS SOLUÇÕES não serão usados para fins diferentes daqueles para os quais foram coletados.

Dados pessoais de funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados.

1. **PROGRAMAS ILEGAIS**

É terminantemente proibido o uso de programas ilegais (software pirata) na EGGS SOLUÇÕES. Os usuários não podem, em hipótese alguma, instalar este tipo de programa nos equipamentos da empresa.

Periodicamente, o Grupo Gestor da Segurança da Informação da EGGS SOLUÇÕES fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.

1. **ADMISSÃO/DEMISSÃO DE COLABORADORES**

O setor de RH da EGGS SOLUÇÕES deverá informar ao Grupo Gestor da Segurança da Informação da EGGS SOLUÇÕES toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou descadastrados nos sistemas da empresa. O RH deverá questionar ao setor responsável pela contratação quais sistemas e repositórios de arquivos de trabalho o novo colaborador deverá ter direito de acesso. Essas informações deverão ser registradas e encaminhadas para o Grupo Gestor da Segurança da Informação através comunicado via e-mail corporativo.

O Grupo Gestor da Segurança da Informação da EGGS SOLUÇÕES fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, que deverá ser trocada pelo usuário no seu primeiro acesso.

No caso de desligamento, o setor de RH deverá comunicar o fato na mesma data ao Grupo Gestor da Segurança da Informação, por meio de e-mail corporativo para que todos os acessos concedidos sejam revogados.

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 EGGS SOLUÇÕES.

1. **CONCESSÃO E REVOGAÇÃO DE ACESSOS**

Quando houver necessidade de concessão ou revogação de acesso aos sistemas, repositórios de arquivos de trabalho e/ou equipamentos de informática da EGGS SOLUÇÕES, o setor solicitante comunicará esta necessidade ao Grupo Gestor da Segurança da Informação da EGGS SOLUÇÕES, copiando o RH, por meio do e-mail corporativo.

1. **POLÍTICA DE SENHAS**

Recomendamos que as senhas tenham sempre no mínimo de 8 (oito) caracteres alfanuméricos, contendo pelo menos uma letra maiúscula e um caractere especial.

Recomendamos que as senhas também sejam ser trocadas pelos usuários a cada 3 meses, não devendo se repetir as senhas definidas nos últimos 12 meses.

Sempre que um usuário é desligado da organização, todas as suas senhas e acessos são revogados no mesmo dia.

1. **ARQUIVOS DE TRABALHO**

Os arquivos de trabalho, considerados dados essenciais ao desenvolvimento do negócio, são mantidos nos servidores de arquivos da EGGS SOLUÇÕES em sistema que permite o controle, comparação e gestão de diferentes versões, denominado SVN. Seu acesso é realizado através de aplicativo VPN do sistema de versionamento homologado pelo Grupo Gestor da Segurança da Informação da EGGS SOLUÇÕES.

São exemplos de arquivos de trabalho:

- Planilha de faturamento;
- Notas fiscais;
- Propostas comerciais;
- Relatórios de análise técnica;
- Planilhas de medição;
- Documentação de sistema utilizada como insumo para o trabalho de análise e medição.

O acesso ao servidor fora das dependências da EGGS SOLUÇÕES é bloqueado e proibido, salvo se realizado através de VPN, com a devida permissão do Grupo Gestor da Segurança da Informação.

1. **ARQUIVOS INDIVIDUAIS**

São considerados arquivos individuais aqueles criados, copiados ou desenvolvidos pelos usuários, que não sejam parte integrante do produto entregável pelo seu trabalho, seja ele interno ou para clientes. Alguns exemplos são: rascunhos ou lembretes, memórias de cálculo, mensagens, diagramas ou instruções técnicas. A cópia de segurança destes arquivos é de responsabilidade dos próprios usuários.

Não é permitido aos usuários o uso ou armazenamento dos tipos de arquivos abaixo relacionados em suas estações de trabalho:

- Programas não licenciados ou não homologados para uso na EGGS;
- Músicas, filmes, séries, programas de TV;
- Vídeos não relacionados à atividade profissional;
- Conteúdo pornográfico ou relacionado a sexo.

1. **COMPARTILHAMENTO DE PASTAS E DADOS**

O compartilhamento de pastas e arquivos de trabalho cujo conteúdo seja classificado como sendo de informação **CONFIDENCIAL** ou **RESTRITA** é proibido através os seguintes:

- Google Talk, WhatsApp, Viber ou qualquer outro comunicador de mensagens instantâneas;
- Compartilhamento de pastas do Windows;
- Bluetooth;
- Cópia via pen drive ou qualquer outro dispositivo removível;
- Google Drive, Dropbox, iCloud, OneDrive ou qualquer outro drive virtual.

Havendo necessidade de se realizar o compartilhamento de dados entre usuários (internos e/ou externos), deve-se utilizar o sistema Pydio.

1. **CÓPIAS DE SEGURANÇA, RECUPERAÇÃO E INTEGRIDADE DOS SISTEMAS E DE SEUS BANCOS DE DADOS**

Cópias de segurança dos sistemas, repositórios de arquivos de trabalho, bancos de dados e configurações dos equipamentos e servidores de rede são de responsabilidade exclusiva do Grupo Gestor da Segurança da Informação.

1. **USO DA INTERNET**

O uso da Internet será monitorado pelo Grupo Gestor da Segurança da Informação, através do uso de sistema de registro de navegação que informa qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

A definição dos funcionários que terão permissão para uso (navegação) de sites restritos, como por exemplo, redes sociais, é atribuição da administração da empresa, a partir da solicitação de seu Gerente/Supervisor.

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:

- estações de rádio (*);
- De jogos on-line;
- De conteúdo pornográfico ou relacionados 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 relacionados aos negócios da EGGS SOLUÇÕES, que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.

Qualquer acesso às redes sociais que não seja relacionado com a área de interesse da empresa não é permitido e, sendo assim, passível de punição.

O acesso a estações de rádio ou ao Spotify é permitido somente para uso via telefone celular, através de conexão estabelecida na rede wi-fi "Convidado".

1. **USO DO CORREIO ELETRÔNICO – ("e-mail corporativo")**

O correio eletrônico fornecido pela EGGS SOLUÇÕES é um instrumento de comunicação interna e externa para a realização dos negócios da empresa.

As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da EGGS SOLUÇÕES, não podem ser contrárias à legislação vigente e nem aos princípios éticos estabelecidos no "Código de Ética e Conduta".

O uso do correio eletrônico é e o usuário é responsável por toda mensagem enviada pelo seu endereço.

Não é permitido o cadastro de contatos pessoais nos sistemas de mensagens instantâneas (ao utilizar a conta profissional @eggs.com.br ou @eggsgestao.com.br); e nem a utilização de contas pessoais.

É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis;
- Sejam relativas a "correntes", de conteúdos pornográficos ou equivalentes;

- Possam prejudicar a imagem da EGGS e/ou de outras empresas;
- Sejam incoerentes com as políticas estabelecidas no “Código de Ética e Conduta” da EGGS SOLUÇÕES.

Não será permitido o uso de e-mail gratuitos (Gmail, Yahoo!, Hotmail, etc.), nos computadores da EGGS.

O Grupo Gestor da Segurança da Informação poderá, visando evitar a entrada de vírus nos computadores da EGGS, bloquear o recebimento de e-mails provenientes de e-mails gratuitos.

1. **NECESSIDADES DE NOVOS SISTEMAS, APLICATIVOS E/OU EQUIPAMENTOS**

O Grupo Gestor da Segurança da Informação é responsável pela definição de compra, substituição e instalação de todo e qualquer “software” e “hardware”.

Qualquer necessidade de novo “software” ou “hardware” deverá ser discutida com os responsáveis pelo Grupo Gestor da Segurança da Informação. Não é permitida a compra ou o desenvolvimento de “softwares” diretamente pelos usuários.

1. **USO DE EQUIPAMENTOS DE PROPRIEDADE DA EMPRESA**

Os usuários que estiverem de posse de qualquer equipamento (desktop, notebook, celular ou tablet) de propriedade da **EGGS SOLUÇÕES IMOBILIÁRIAS/BR 153 Loteamento Empresaria**.

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;
- O usuário não deve instalar ou remover nenhum programa do equipamento recebido. Também não deve alterar a configuração de nenhum programa previamente instalado.

Fora do trabalho:

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e 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 furto

- Registre a ocorrência em uma delegacia de polícia;
- Comunique o fato o mais rápido possível ao seu superior imediato e ao Grupo Gestor da Segurança da Informação;
- Envie uma cópia do boletim de ocorrência para o RH.

1. **RESPONSABILIDADES DOS GERENTES/SUPERVISORES**

Os gerentes e supervisores são responsáveis pelas definições dos direitos de acesso de seus subordinados aos sistemas e informações da empresa, cabendo a eles verificarem se eles estão acessando exatamente os sistemas e as áreas de dados 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 Grupo Gestor da Segurança da Informação fará auditorias periódicas do acesso dos usuários às informações, verificando:

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

1. **SISTEMA DE TELECOMUNICAÇÕES**

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da **EGGS SOLUÇÕES IMOBILIÁRIAS/BR 153 Loteamento Empresaria**.

, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do Grupo Gestor da Segurança da Informação, de acordo com as definições da administração da empresa.

1. **USO DE ANTIVÍRUS**

Todo arquivo obtido através da Internet ou recebido de entidade externa a EGGS SOLUÇÕES deve ser verificada por programa antivírus.

Todas as estações de trabalho possuem software antivírus instalado. A sua atualização será automática, agendada pelo Grupo Gestor da Segurança da Informação, via rede.

O usuário não pode, em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

9. **VIOLAÇÃO DA POLÍTICA DE SEGURANÇA**

É qualquer ato que:

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

10. **PENALIDADES**

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

Vigência

O disposto no presente documento entrará em vigor na data de publicação do comunicado que o anunciar.