Política de Uso Aceitável de Ativos de Informação e Equipamentos Tecnológicos

Grupo Edson Queiroz

#### ÍNDICE

[1. APRESENTAÇÃO 3](#_Toc143096949)

[1.1. Objetivo 3](#_Toc143096950)

[1.2. Abrangência 3](#_Toc143096951)

[1.3. Vigência 3](#_Toc143096952)

[1.4. Área técnica responsável pela política 3](#_Toc143096953)

[1.5. Aprovação 3](#_Toc143096954)

[2. CONCEITOS E DEFINIÇÕES 4](#_Toc143096955)

[3. DOCUMENTOS DE REFERÊNCIA 5](#_Toc143096956)

[4. DIRETRIZES 6](#_Toc143096957)

[4.1. Gerais 6](#_Toc143096958)

[4.2. Uso de equipamento tecnológico 6](#_Toc143096959)

[4.3. Dispositivo de armazenamento móvel 7](#_Toc143096960)

[4.4. Armazenamento em nuvem 7](#_Toc143096961)

[4.5. Certificação digital 7](#_Toc143096962)

[4.6. Uso de equipamentos por terceiros 7](#_Toc143096963)

[4.7. Equipamentos de impressão e reprografia (fotocopiadoras) 8](#_Toc143096964)

[4.8. Áreas seguras 8](#_Toc143096965)

[5. DIVULGAÇÃO E DISSEMINAÇÃO 8](#_Toc143096966)

[6. CONSEQUÊNCIAS 9](#_Toc143096967)

[7. RESPONSABILIDADES 9](#_Toc143096968)

[7.1. Área de Operações de Infraestrutura de TI 9](#_Toc143096969)

[7.2. Área de Segurança da informação 9](#_Toc143096970)

[7.3. Colaboradores 10](#_Toc143096971)

[8. EXCEÇÕES 10](#_Toc143096972)

# APRESENTAÇÃO

## Objetivo

Esta política tem por objetivo estabelecer as diretrizes para o uso de ativos de informação e de equipamentos tecnológicos do Grupo Edson Queiroz (GEQ).

## Abrangência

Esta política é aplicável a todas as empresas do GEQ.

## Vigência

Esta política terá prazo indeterminado e entrará em vigor a partir da data de sua publicação, com revisão periódica a cada 12 (doze) meses ou quando for necessária.

## Área técnica responsável pela política

O conteúdo dessa política é de responsabilidade da área de Operações de Infraestrutura de Tecnologia da Informação (TI).

## Aprovação

|  |  |  |
| --- | --- | --- |
| Carlos Rotella | Presidente Executivo |  |
| Ivens Medeiros | Gerente Jurídico |  |
| Aleksandro Oliveira | *Chief Financial Officer (CFO)* |  |
| Elber Reis | Diretor de TI |  |

# CONCEITOS E DEFINIÇÕES

* **Área segura:** ambientes de processamento das informações críticas ou sensíveis do GEQ, os quais são protegidos contra ameaças à segurança (infiltrações, vazamento de água proveniente de outra área, etc).
* **Ativo de informação:** patrimônio intangível do GEQ, constituído por informações de qualquer natureza (estratégica, técnica, administrativa, financeira, mercadológica, de recursos humanos e/ou legal), incluindo aquelas criadas ou adquiridas de forma legal e sem conflito e/ou infração a eventuais acordos de confidencialidade vigentes por meio de parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico, eletrônico ou digitalizado.
* **Altos Executivos:** empregados que exercem a função de Diretor Superintendente, Diretor Executivo, Diretor Corporativo ou Diretor de Negócio.
* **Certificado Digital:** tecnologia de identificação que permite que transações eletrônicas dos mais diversos tipos sejam feitas considerando sua integridade, sua autenticidade e sua confidencialidade, de forma a evitar que adulterações, interceptações ou outros tipos de fraude ocorram.
* **Colaborador:** inclui empregados, estagiários, temporários e terceiros vinculados às empresas do GEQ.
* **Comitê Gestor de Segurança da Informação (CGSI):** grupo de trabalho multidisciplinar permanente, efetivado pela diretoria do GEQ, que tem por finalidade tratar questões ligadas à Segurança da Informação.
* **Confidencialidade:** é um princípio fundamental de sigilo, ou seja, que não permite a divulgação de dados da empresa para indivíduos, entidades ou processos sem autorização.
* **Controle:** medida de segurança para o tratamento de um risco específico.
* **Disponibilidade:** propriedade ou permissão de utilização dos ativos do GEQ de serem acessíveis e utilizáveis sob demanda, por portas autorizadas.
* **Dispositivos móveis:** são usados para realizar armazenamento, processamento e transmissão de informações, que permite ao usuário mobilidade inclusive fora do ambiente corporativo. Exemplo: celulares, notebooks, tablets, coletor de dados etc.
* **Equipamento tecnológico:** equipamentos usados para cumprir funções, armazenar documentos, fazer pesquisas, agregar software, entre outros.
* **Incidente de segurança da informação:** qualquer ocorrência de evento que viole os princípios de segurança da informação (confidencialidade, integridade, disponibilidade e autenticidade) do GEQ ou de terceiros com os quais o GEQ comprometeu-se com a manutenção da segurança dos dados.
* **Integridade:** propriedade dos ativos da informação do GEQ de serem precisos, consistentes e completos.
* **Segurança da informação:** competência que visa proteger a informação contra ameaças e vulnerabilidades buscando garantir a continuidade do negócio e minimização de riscos, alinhado com os objetivos estratégicos de negócio. Adicionalmente, zela pelos princípios de confidencialidade, integridade, disponibilidade e autenticidade das informações do GEQ ou de terceiros sob a sua guarda.

# DOCUMENTOS DE REFERÊNCIA

Esta política possui inter-relacionamento e/ou faz referência aos seguintes documentos:

* Código de Conduta.
* Contrato de Trabalho
* Lei nº 13.709/18 (Lei Geral de Proteção de Dados)
* Política de Acesso a Ambientes de Data Center
* Política de Acesso à Internet e Comportamento em Mídias Sociais
* Política de Ativo Fixo
* Política de Benefícios para Altos Executivos
* Política de Consequências
* Política de Gestão de Identidade e Controle de Acessos
* Política de Rescisão
* Política de Segurança da Informação

# DIRETRIZES

## Gerais

* + 1. Os equipamentos tecnológicos disponibilizados aos colaboradores são para uso exclusivo em suas atividades profissionais, podem ser (mas não são limitados a):

1. Computadores (equipamentos, arquivos e aplicações);
2. Senhas de segurança (chaves e cartões de acesso);
3. Dispositivos móveis (incluindo telefone celular);
4. Impressoras, scanners e qualquer outro equipamento digital.
   * 1. É expressamente proibida a utilização dos equipamentos tecnológicos da empresa para fins particulares.
     2. Os equipamentos tecnológicos somente devem ser disponibilizados a colaboradores mediante assinatura de Termo de Responsabilidade, conforme previsto na Política de Ativo Fixo.
     3. A cessão e responsabilidade de equipamentos tecnológicos cedidos ao uso temporários de terceiros (não empregados) deve ser tratado no âmbito do contrato de prestação de serviços com a empresa contratada, conforme determina a Política de Ativo fixo.
     4. O uso de equipamentos tecnológicos deve seguir as diretrizes previstas no Código de Conduta, na Política de Segurança da Informação e na Política de Ativo Fixo.

## Uso de equipamento tecnológico

* + 1. A manutenção e/ou modificação de quaisquer equipamentos tecnológicos é uma atribuição específica da área de Operações de Infraestrutura de TI que, a seu exclusivo critério, pode delegar formalmente outro responsável. Os demais usuários são expressamente proibidos de realizar qualquer tipo de manutenção e/ou modificação nos equipamentos.
    2. Os equipamentos tecnológicos devem conter somente softwares homologados pela área de Segurança da Informação de TI.
    3. Ao final do contrato de trabalho ou da prestação de serviços, os equipamentos disponibilizados devem ser devolvidos em sua totalidade e em adequado estado de conservação. Para os Altos Executivos, devem ser observadas as diretrizes da Política de Benefícios para Altos Executivos.
    4. Os equipamentos (computadores e celulares) de ex-colaboradores devem ser submetidos a um processo de sanitização das informações corporativas.
    5. Qualquer dano aos equipamentos tecnológicos deve ser devidamente analisado e havendo a constatação de que o dano é resultante de qualquer conduta dolosa ou culposa, cabe ao GEQ exercer seu direito de reparação, bem como adotar as medidas estabelecidas no Contrato de Trabalho ou Contrato de Prestação de Serviço e na Política de Consequências.

## Dispositivo de armazenamento móvel

* + 1. É proibido o uso de dispositivos de armazenamento móvel (HDs externos, pendrives, etc.) em desktops, notebooks e servidores ou em quaisquer equipamentos do GEQ.

## Armazenamento em nuvem

* + 1. Sempre que necessário, deve ser disponibilizado para os colaboradores espaço para armazenamento de arquivos em nuvem através de solução corporativa aprovada pela área de Operações de Infraestrutura de TI e homologada pela área de Segurança da Informação.
    2. Qualquer utilização ou tentativa de utilização de solução de armazenamento em nuvem não homologada pela área de Segurança de Informação é considerado uma violação de segurança da informação.

## Certificação digital

* + 1. Certificados digitais podem ser fornecidos, a exclusivo critério do GEQ, para os colaboradores cuja atividades necessitem de sua utilização.
    2. Os custos dos certificados digitais devem ser de responsabilidade exclusiva da área solicitante.
    3. Os colaboradores que utilizarem certificado digital fornecido pela empresa devem seguir as seguintes recomendações:

1. Conservar o certificado digital, independentemente do equipamento que o suporte, bem como zelar pela guarda e sigilo de sua respectiva senha ou meio de autenticação;
2. Informar a área de Segurança da Informação sobre quaisquer eventos ou suspeitas relativas à integridade de sua senha e/ou ao uso indevido do certificado digital.

## Uso de equipamentos por terceiros

* + 1. A conexão de terceiros na rede WiFi deve ser solicitada formalmente e somente deve ser fornecida por tempo determinado e em rede segmentada.
    2. A rede de acesso a equipamentos de terceiros deve seguir o mesmo monitoramento e políticas das demais redes do GEQ.
    3. Em caso de acesso à rede WiFi do GEQ, não poderá o terceiro efetuar o *download* de nenhum *software* sem o conhecimento, autorização e homologação prévia da área de Segurança da Informação da TI.
    4. Os consultores terceiros devem utilizar somente equipamentos da empresa que presta serviço (empresa contratada pelo GEQ) e que cumpram os requisitos de segurança do GEQ. Não é permitido o uso de equipamentos pessoais pelos consultores terceiros.
    5. O suporte, atualização, manutenção, reposição de peças, licenciamento de softwares, reembolso ou qualquer outro tipo de gasto referente ao uso de dispositivos e de recursos computacionais de terceiros não devem ser custeados pelo GEQ.

## Equipamentos de impressão e reprografia (fotocopiadoras)

* + 1. O uso de equipamentos de impressão e reprografia (fotocopiadoras) deve ser feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse do GEQ ou que estejam relacionados com o desempenho das atividades profissionais do colaborador.

## Áreas seguras

* + 1. O GEQ pode reconduzir o mapeamento de áreas relacionadas à manipulação de informações críticas ou sensíveis, assim como definir novos controles de acesso que se façam necessários, caso sejam identificadas ameaças e vulnerabilidades da segurança física das áreas seguras.
    2. Não é permitido consumir qualquer tipo de alimento, bebida ou uso de produto fumígeno em áreas apontadas como sensíveis no GEQ.
    3. Os ambientes físicos podem ser monitorados com o uso de sistema de circuito fechado de televisão (CFTV) em áreas comuns e as imagens obtidas devem ser armazenadas e protegidas contra qualquer tipo de manipulação não autorizada. O armazenamento das imagens deve seguir os princípios da Lei Geral de Proteção de Dados.

# DIVULGAÇÃO E DISSEMINAÇÃO

A divulgação interna e disseminação desta política é fundamental para sua efetividade. Cabe à área técnica responsável desenvolver periodicamente planos de comunicação e treinamento para disseminação desta política, seja para a totalidade dos colaboradores ou para grupos específicos, conforme a necessidade e/ou confidencialidade do tema.

# CONSEQUÊNCIAS

A violação dessa política sujeitará o infrator às medidas previstas no Código de Conduta e na Política de Consequências.

O conhecimento de qualquer infração ou indício de infração das regras contidas nesta política deve ser relatada no Canal de Conduta, disponível 24 horas por dia, 7 dias por semana, pelo número 0800-602-1836, pela internet ([www.contatoseguro.com.br/grupoedsonqueiroz](http://www.contatoseguro.com.br/grupoedsonqueiroz)) ou pelo aplicativo de celular da Contato Seguro.

Todos os relatos são direcionados ao Comitê de Conduta e tratados de forma confidencial. Não é admitida, sob qualquer circunstância, retaliação ou represália ao colaborador ou outra pessoa que utilizar apropriadamente o Canal de Conduta.

# RESPONSABILIDADES

## Área de Operações de Infraestrutura de TI

1. Realizar a alteração e/ou manutenção de qualquer equipamento tecnológico disponibilizado pelo Grupo Edson Queiroz;
2. Realizar a instalação de ferramentas de proteção para dispositivos de armazenamento móveis;
3. Realizar sanitização dos equipamentos tecnológicos nos casos de desligamento de colaboradores;
4. Analisar quaisquer danos com equipamentos tecnológicos, conforme item 4.2.5;
5. Aprovar solução corporativa para armazenamento em nuvem, conforme item 4.4.1.

## Área de Segurança da informação

1. Definir estratégias e tecnologias de segurança para o uso, controle, monitoramento e remediação de ativos de tecnologia;
2. Garantir a criação e atualização dos procedimentos complementares a esta política;
3. Monitorar e reportar a CGSI, ao CFO e ao Diretor de TI anomalias no cumprimento dessa política;
4. Comunicar ao Gestor de Segurança da Informação eventuais tentativas de desvio de conduta dos termos desta política.

## Colaboradores

1. Realizar a assinatura do Termo de Responsabilidade quando receber equipamentos tecnológicos para as atividades laborais;
2. Realizar a devolução dos equipamentos tecnológicos em perfeito estado de conservação, ressalvados os desgastes naturais do uso, quando do seu desligamento;
3. Comunicar ao Departamento de Tecnologia da Informação sobre alguma possível anomalia nos ativos de tecnologia sob sua responsabilidade.

# EXCEÇÕES

Para todas as situações excepcionais e/ou não contempladas nesta política caberá ao Diretor de Tecnologia da Informação e ao *Chief Financial Officer* (CFO) tomar a decisão emergencial sobre a medida a ser adotada e, caso necessário, solicitar a sua posterior inclusão nesta política.

\* \* \*