Política da Segurança da Informação

Grupo Edson Queiroz

#### 

#### ÍNDICE

[1. APRESENTAÇÃO 3](#_Toc328671088)

[1.1. Objetivo 3](#_Toc328671089)

[1.2. Abrangência 3](#_Toc328671090)

[1.3. Vigência 3](#_Toc328671091)

[1.4. Área técnica responsável pela política 3](#_Toc328671092)

[1.5. Comitê da Segurança da Informação 3](#_Toc328671093)

[1.6. Aprovação 3](#_Toc328671093)

[2. CONCEITOS E DEFINIÇÕES 4](#_Toc328671094)

[3. DOCUMENTOS DE REFERÊNCIA 6](#_Toc328671095)

[4. DIRETRIZES 6](#_Toc328671096)

[4.1. Gerais 6](#_Toc328671097)

[4.2. Responsabilidades](#_Toc328671098) 9

[4.3. Gestão de Acesso](#_Toc328671098) 10

[4.4. Correio Eletrônico(Solução de Colaboração)](#_Toc328671099) 11

[4.5. Internet](#_Toc328671098) 11

[4.6. Acesso Remoto (VPN)](#_Toc328671098) 11

[4.7. Sanções](#_Toc328671098) 12

5. Exceções 12

1. APRESENTAÇÃO

## **Objetivo**

Esta política tem o objetivo de estabelecer as diretrizes relacionadas à segurança física e lógica das informações do Grupo Edson Queiroz, e garantir a confidencialidade, integridade, disponibilidade, autenticidade, responsabilidade, auditabilidade, legalidade e não repúdio, independente do meio de armazenamento, processamento ou transmissão que seja utilizado.

## **Abrangência**

Aplicável a todas as unidades de negócios do Grupo Edson Queiroz.

## **Vigência**

Esta Política terá prazo indeterminado e entrará em vigor a partir da data de sua publicação, com revisão periódica a cada 6 meses ou quando for necessária.

## **Área técnica responsável pela política**

O conteúdo dessa política é de responsabilidade da Gerência Geral de TI.

## **Aprovação**

|  |  |  |
| --- | --- | --- |
| Abelardo Rocha | Diretoria Executiva |  |
| Edson Queiroz Neto | Diretoria Executiva |  |
| Igor Barroso | Diretoria Executiva |  |
| Aélio Silveira | Gerente Geral de TI |  |

1. CONCEITOS E DEFINIÇÕES

* *Ativos:* é tudo aquilo que tenha valor para empresa. Tais como: ativos de informação, de software e físicos, além de intangíveis (imagem e reputação), serviços, pessoas.
* *Autenticação:* procedimento para determinar a identidade de um colaborador que esteja tentando acessar um sistema.
* *Autenticidade:* propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.
* *Backup:* termo em inglês que tem o significado de cópia de segurança.
* *Chave de Acesso:* identificação única através de símbolos ou uma sequência de caracteres usada para identificar um colaborador.
* *Colaborador:* a palavra “COLABORADOR” inclui o Diretor Executivo, Diretores, Gestores, demais Empregados, Estagiários, Temporários e Terceiros vinculados às Empresas do GEQ.
* *Confidencialidade:* propriedade que limita o acesso a informação tão somente às pessoas devidamente autorizadas, ou seja, àquelas tem a permissão concedida pelo proprietário da informação.
* *Data Center:* é o local onde são concentrados os equipamentos de processamento e armazenamento de dados de uma empresa ou organização. Também conhecido como CPD - Centro de Processamento de Dados.
* *Desastres lógicos e físicos:* são desastres que podem causar interrupção nos sistemas e na continuidade dos negócios, e geralmente são ocasionados por: incêndio, enchente, terremoto, furacão, interrupção do fornecimento de energia elétrica, sobrecargas elétricas, sabotagem, fraudes, acessos não autorizados e dentre outros.
* *Disponibilidade:* propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (início, manutenção e destruição).
* *Dispositivos móveis:* celulares, notebooks, *tablets*, coletor de dados, etc.
* *Gestor:* Gerentes, Superintendentes, Diretores.
* *GEQ:* Grupo Edson Queiroz.
* *Informação:* é um ativo que, como outro qualquer ativo importante para os negócios, tem um valor para a organização e consequentemente necessita ser adequadamente protegido.
* *Integridade:* é a propriedade que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.
* *Internet:* rede mundial que interliga computadores em todo o mundo.
* *Intranet:* rede privada dentro de uma organização que está de acordo com os mesmos padrões da Internet, acessível apenas por membros da organização, empregados ou terceiros com autorização de acesso.
* *Log:* são registros cronológicos de atividades do sistema que possibilitam a reconstrução, revisão e análise dos ambientes e atividades relativas a uma operação, procedimento ou evento, acompanhados do início ao fim.
* *Não repúdio:* garantir que a transação não pode ser negada aos colaboradores após o acesso.
* *Recursos computacionais:* são entendidos como computadores, notebooks, equipamentos de rede, cabeamento, sistemas, softwares, informações/dados e demais dispositivos integrantes a TI.
* Responsabilidade: comprometimento dos colaboradores com a integridade da informação e com os ativos da organização.
* *Solução de colaboração:* correio eletrônico (“e-mail”), Calendário, Agenda, Comunicador Instantâneo, Office Web, Disco Virtual, etc.
* *Superusuário:* conta de usuário com poder de administrador do sistema. Possui acesso total ao sistema.
* *TI:* Tecnologia da Informação.
* *Unidade de negócio:* corresponde a cada empresa do Grupo Edson Queiroz, englobando o conjunto de suas respectivas matrizes e filiais.
* *VPN (Virtual Private Network – Rede Privada Virtual):* é um sistema que permite o acesso privado de comunicação, utilizando de redes públicas já existentes, como por exemplo, a Internet.

1. DOCUMENTOS DE REFERÊNCIA

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

* Código de Conduta;
* NBR ISSO/IEC 27002;
* Normas da Segurança da Informação;
* Procedimentos da Segurança da Informação;
* Política de Ativo Fixo.

1. DIRETRIZES

## **Gerais**

* + 1. O Comitê de Segurança da Informação é um grupo multidisciplinar, aprovado pela Diretoria Executiva que será composto pelo menos por um integrante de cada uma das seguintes áreas: Gerência de Operações e Infraestrutura, Auditoria, Recursos Humanos e Jurídico.
    2. A segurança da informação deve ser prioridade em todos os processos implantados, e projetada de forma eficaz nos novos empreendimentos.
    3. A informação é um ativo da empresa que não deve ser alterada, acessada e/ou destruída indevidamente.
    4. Todas as instalações físicas, recursos computacionais e informações nestas armazenadas, processadas e/ou criadas, são de propriedade do GEQ, que podem ser monitorados e auditados, bem como os seus acessos e as suas utilizações.
    5. Os equipamentos, sistemas e serviços de rede fornecidos pelas unidades organizacionais do GEQ são para o exercício das funções de seus colaboradores para o uso corporativo, sendo vedada sua utilização para fins pessoais.
    6. Todos os recursos computacionais do GEQ devem estar adequadamente legalizados e em conformidade com as normas vinculadas a esta Política.
    7. É proibido divulgar informações e imagens de propriedade do GEQ ou que estejam sob sua custódia sem autorização prévia do responsável pela informação.
    8. Os incidentes de segurança devem ser identificados, monitorados, comunicados e devidamente tratados.
    9. Todo incidente de segurança da informação deve ser reportado ao e-mail: [seginfo.ti@edsonqueiroz.com.br](mailto:seginfo.ti@edsonqueiroz.com.br), para o devido registro e as providências adequadas.
    10. Toda informação confidencial deve ser armazenada ou transmitida de forma segura, garantindo a integridade e a confidencialidade.
    11. Devem ser mantidas cópias de segurança dos sistemas e informações corporativas, periodicidade e mecanismo de armazenamento adequado, conforme a norma e o procedimento de Backup, para a proteção dos dados corporativos mesmo em eventual ocorrência de incidente que resulte em destruição completa de um dos Data Centers do GEQ.
    12. Todas as alterações nos sistemas do GEQ devem ser realizadas em ambientes de desenvolvimento e testadas em ambientes de homologação, antes de serem implantadas no ambiente de produção, serão aprovadas pelo comitê de Gestão de Mudanças de TI.
    13. Todos os sistemas e recursos computacionais devem estar livres de vulnerabilidades que possam comprometer a Segurança das Informações.
    14. Todos os colaboradores que utilizarem os dispositivos móveis de propriedade do GEQ são responsáveis pelos equipamentos e as atualizações dos aplicativos que forem necessárias.
    15. O bloqueio através de senha deve ser utilizado em todos os dispositivos móveis que possuírem tal recurso.
    16. A seu exclusivo critério e conveniência, a área de TI poderá monitorar e auditar a utilização dos equipamentos, arquivos armazenados e a utilização dos equipamentos corporativos.
    17. Deverão ser mantidos registros de todas as ações executadas em equipamentos do GEQ que possam ser necessárias para fins de auditoria, verificação e investigação de violações à Política de Segurança da Informação, suas normas e procedimentos, para garantir o atendimento de requisitos legais e ordens judiciais.

## **Responsabilidades**

* + 1. Colaboradores
       1. Todo colaborador deve conhecer e seguir a Política de Segurança da Informação, suas Normas e os Procedimentos.
       2. Todos os colaboradores que possuam acesso ou utilizam os recursos computacionais do GEQ, devem estar conscientes dos limites que existem para o uso das informações e dos ativos associados ao GEQ, além de serem responsáveis pelo uso de quaisquer recursos de processamento da informação e quaisquer outros usos conduzidos sob as suas responsabilidades.
       3. Não enviar, armazenar e/ou manusear material que caracterize: promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas; assuntos de caráter obsceno, prática de qualquer tipo de discriminação relativa à raça, sexo ou credo religioso; distribuição de qualquer material que caracterize pornografia, pedofilia, atentado ao pudor, violação de direito autoral garantido por lei.
       4. Em caso de roubo, dano ou perda de todos os dispositivos de TI, o colaborador deverá seguir o que estabelece no item 4.12 da Política de Ativo Fixo.
    2. Área de Tecnologia da Informação
       1. Adotar medidas para detectar e coibir o uso não autorizado e inadequado de credenciais administrativas (ou com privilégios “super-usuário”), assegurando a proteção adequada dos ativos sob sua custódia.
       2. Todos os tipos de acessos solicitados devem ser liberados somente após a autorização do gestor responsável.
       3. Manter arquivos de *log* para registrar ações dos colaboradores, com o objetivo de serem fontes de informação para auditorias futuras.
       4. Detectar, identificar, registrar as violações ou tentativas relevantes e significativas de acesso não autorizadas.
       5. Devem controlar e monitorar para que os recursos tecnológicos, de infraestrutura e os ambientes físicos utilizados para suportar os sistemas de informação tenham controle de acesso físico, condições ambientais adequadas e que devam ser protegidos contra situações e indisponibilidade causadas por desastres e contingências.
       6. Garantir a continuidade dos sistemas, equipamentos e recursos críticos para os negócios das unidades organizacionais do GEQ, além de, assegurar que a Política da Segurança da Informação, suas normas e procedimentos sejam cumpridos.
    3. Recursos Humanos/Gestão de Pessoas
       1. Assegurar de que os colaboradores e prestadores de serviços sejam treinados, orientados sobre a existência desta Política, suas normas e procedimentos, e comprovem por escrito, o conhecimento destas.
       2. Adotar os procedimentos e mecanismos existentes para comunicar à Área de Tecnologia de Informação (TI) e da Segurança da Informação todos os desligamentos, afastamentos, licenças, férias e modificações no quadro funcional das unidades organizacionais do GEQ.
    4. Comitê de Segurança da Informação
       1. Tratar de temas de Segurança da Informação e analisar soluções específicas.
       2. Explicar ou decidir sobre pontos omissos que necessitem de esclarecimentos desta Política, suas normas e procedimentos, submetendo-os à aprovação da Diretoria Executiva com o auxílio da Gestão de Políticas.
       3. Analisar alterações na Política da Segurança da Informação, suas normas e procedimentos.

## **Gestão de acesso**

* + 1. Os controles de acesso físicos ou lógicos têm como objetivo proteger equipamentos, locais físicos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada.
    2. A autorização, o acesso, o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada colaboradores, e qualquer outra forma de uso ou acesso além do necessário depende de prévia autorização do gestor da área responsável pela informação.
    3. O colaborador é responsável por qualquer ação realizada com a sua chave de acesso e as informações as quais estejam sob sua responsabilidade.
    4. Periodicamente os acessos concedidos devem ser revistos pela área responsável.
    5. Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados.
    6. Todos os sistemas de informação do GEQ, devem ter pelo menos um responsável, formalmente designado pelo gestor, que deve definir os privilégios de acesso às informações.
    7. Toda e qualquer alteração de acesso do colaborador deve ser realizada, somente após a aprovação do Gestor Responsável e segundo os critérios definidos nesta Política.

## **Correio Eletrônico (Solução de Colaboração)**

* + 1. A solução de colaboração do GEQ não deve ser utilizada para fins pessoais, pois é uma ferramenta disponibilizada apenas para o uso consciente e exclusivo a assuntos corporativos.
    2. O GEQ, como proprietário da solução de colaboração, poderá a qualquer momento e sem aviso prévio, monitorar o uso desta ferramenta inclusive o conteúdo das mensagens quando julgar necessário.
    3. As mensagens de correio eletrônico são instrumentos de comunicação interna e externa para realização de negócio do GEQ. Elas devem ser escritas em linguagem profissional e que não comprometa a imagem do GEQ.

## **Internet**

* + 1. A Internet e a Intranet devem ser usadas para as atividades profissionais do GEQ.
    2. Endereços da Internet que não agreguem ao GEQ e/ou as atividades corporativas exercidas não devem ser acessados.
    3. O colaborador não deve disponibilizar, na Internet, informações corporativas e pessoais que comprometam o GEQ.
    4. Todo colaborador é responsável pelas ações e acessos realizados por sua conta de acesso (login) na Internet e Intranet.
    5. O acesso a Internet que o GEQ disponibiliza pode ser monitorado, sem aviso prévio, com o objetivo de garantir a segurança da informação, e deve ser utilizado para o desempenho das atividades profissionais.
    6. Não devem ficar armazenados dados, como: “*login”*, senhas em qualquer site acessado.

## **Acesso Remoto**

* + 1. O acesso remoto aos recursos computacionais deve ser realizado adotando os mecanismos de segurança definidos pela área responsável da TI do GEQ, com intuito de evitar ameaças à integridade e sigilo do serviço.
    2. O acesso remoto aos serviços corporativos somente deve ser disponibilizado aos colaboradores que, oficialmente, executem atividade vinculada à assuntos profissionais do GEQ, desde que autorizados pela área responsável, para que se evitem ameaças à integridade e ao sigilo das informações contidas na rede do GEQ.

## **Sanções**

* + 1. No caso de descumprimento ou violação de um ou mais itens da Política de Segurança da Informação, normas, procedimentos ou atividades pertinentes à Segurança da Informação, será aplicado o tratamento previsto no Código de Conduta e na legislação específica.

# EXCEÇÕES

Para todas as situações excepcionais não abarcadas por esta política necessitará a avaliação pelo Comitê de Segurança da Informação para que seja tomada a decisão emergencial sobre a regra a ser adotada e sua posterior inclusão nesta política.