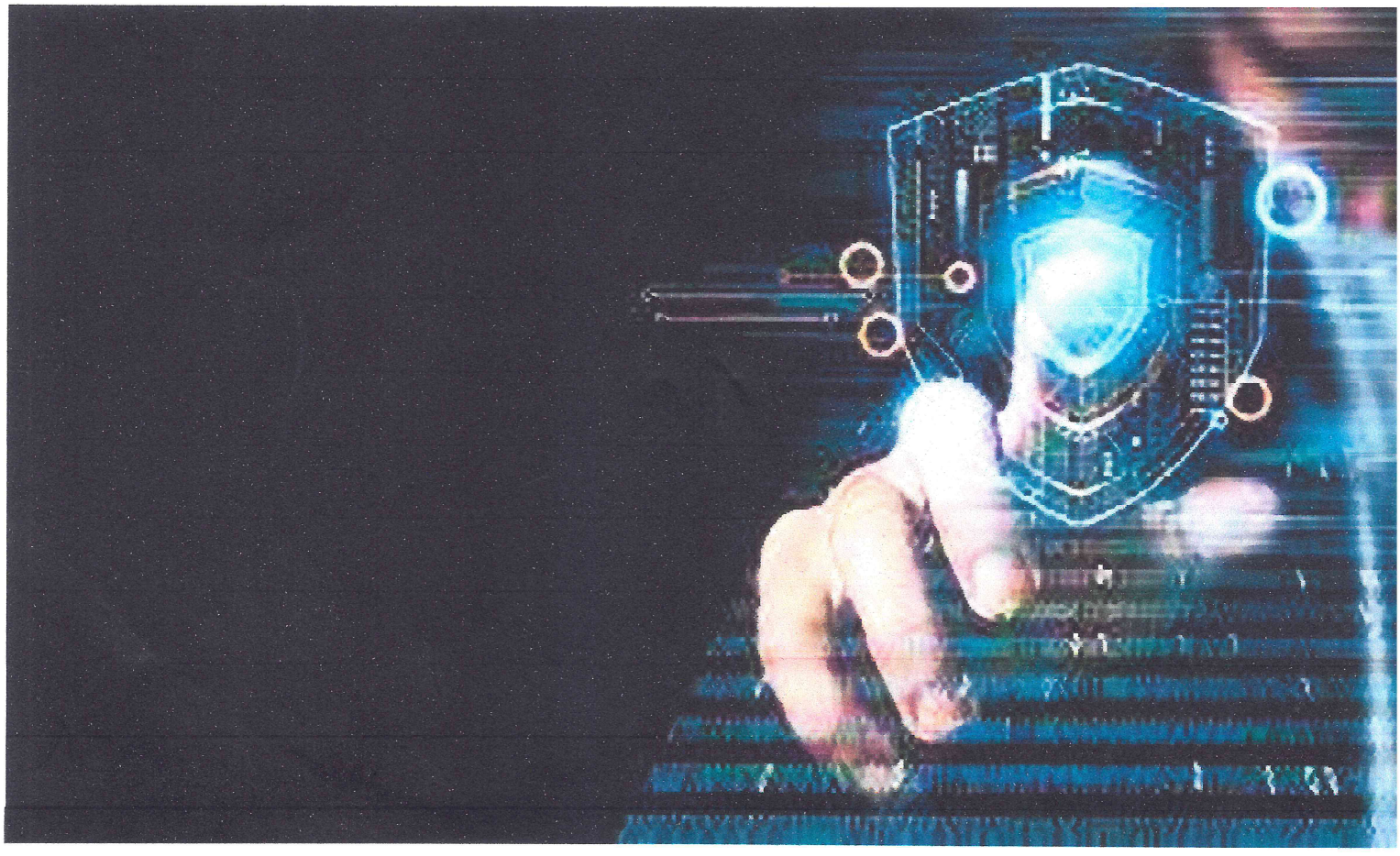
# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



## Histórico de Alterações

| DATA | VERSÃO | AUTOR (A) | DESCRIÇÃO |
|---|---|---|---|
| 11/01/2021 | 1.0 | Alex de Oliveira | Elaboração da política. |
| 19/08/2022 | 1.1 | Érika Aguiar | Adequação da política a normatização da ISO/IEC 27000; 27001; à Lei nº 13.709/2018 e Resolução nº 4893/2021 do Bacen. |
| 03/10/2023 | 1.2 | Érika Aguiar | Adequação da política para todas as empresas do Grupo Globalservice. |
| 18/11/2024 | 1.3 | Érika Aguiar | Revisão da Política de Segurança da Informação. |

**Este documento deve:**

1. Deve passar por revisões anuais ou sempre que houver necessidade;
2. Ter cópia controlada e somente gerada pela área responsável; e
3. Ser divulgado a todos os funcionários, prestadores de serviços, estagiários e afins da organização.


## Aviso Legal

Este material foi elaborado pelo **Grupo Globalservice** em parceria com a empresa **Aguiar Consultoria e Auditoria Contábil Ltda.** O documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações, sob o conhecimento de que qualquer disseminação, distribuição ou cópia deste conteúdo é **proibida**.

**novembro/2024**

## SUMÁRIO

1. INTRODUÇÃO ..... 005

2. ESCOPO ..... 005

3. DOCUMENTOS DE REFERÊNCIA ..... 005

4. OBJETIVOS ..... 005

5. TERMINOLOGIA BÁSICA DA SEGURANÇA DA INFORMAÇÃO ..... 006

6. DIRETRIZES ..... 006

7. SEGURANÇA DA INFORMAÇÃO ..... 007
7.1. Regras de Segurança da Informação ..... 007
7.2. Acesso a Informação ..... 008
7.3. Sistemas ..... 008
7.4. Tratamento da Informação ..... 009
7.5. Recomendações para o Tratamento da Informação ..... 010
7.6. Segurança Quanto às Pessoas ..... 011
7.7. Segurança Lógica de Computadores, Redes e Sistemas Aplicativos ..... 012

8. ADMINISTRAÇÃO DO ACESSO AOS SISTEMAS ..... 012
8.1. Administração do Acesso de Usuários ..... 012
8.2. Controle de Acesso a Computadores e Redes ..... 012
8.3. Monitoramento de Uso e Acesso aos Sistemas ..... 013

9. SEGURANÇA NO ACESSO DE PRESTADORES DE SERVIÇOS ..... 013

10. SEGURANÇA FÍSICA DE COMPUTADORES ..... 013
10.1. Normas para Segurança Física de Computadores ..... 013

11. PRECAUÇÕES ÀS MÍDIAS DE ARMAZENAMENTO ..... 014

12. COMITÊ DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO – CGSI ..... 014

13. BACKUP ..... 014

14. UTILIZAÇÃO SEGURA DE *HARDWARE* E *SOFTWARE* ..... 014

15. SERVIÇOS PORTAL DE CHAMADOS ..... 015

16. ACESSO À INTERNET ..... 015

17. ACESSO AO CORREIO ELETRÔNICO..... 015

18. PLANO DE CONTINUIDADE DO NEGÓCIO..... 016

19. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO..... 016

20. IMPRESSÃO..... 017

21. MESA LIMPA..... 018

22. CLASSIFICAÇÃO DA INFORMAÇÃO..... 018

23. GESTÃO DA IDENTIDADE..... 019

24. ARMAZENAMENTO E DESCARTE DA INFORMAÇÃO FÍSICA..... 020

25. TREINAMENTO..... 020

26. IDENTIFICAÇÃO VISUAL..... 021

27. CERTIFICADO DIGITAL..... 021

28. MONITORAÇÃO E INSPEÇÃO..... 022

29. LGPD..... 022

30. VEDAÇÕES..... 023

31. PAPÉIS E RESPONSABILIDADES..... 025

32. SANÇÕES E PUNIÇÕES..... 028

33. CASOS OMISSOS..... 028

34. DISPOSIÇÕES FINAIS..... 028

35. DISPOSIÇÕES GERAIS..... 029

36. REVISÕES..... 029

37. GESTÃO DA POLÍTICA..... 029

## 1. INTRODUÇÃO

O Grupo Globalservice tem como missão prestar serviços de segurança, agente de portaria e transporte de valores com excelência em qualidade e atendimento, que assegure aos seus clientes segurança, confiança e pontualidade, gerando sólidas relações de longo prazo.

1.1. O Grupo Globalservice entende que a informação corporativa é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos serviços ofertados a seus clientes.

1.2. O Grupo Globalservice compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

1.3. Desta forma, o Grupo Globalservice estabelece sua Política de Segurança da Informação, como parte integrante do seu Sistema de Gestão de Segurança da Informação – SGSI, alinhada às boas práticas e legislações vigentes, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

## 2. ESCOPO

A política aqui estabelecida deve ser cumprida por todas as partes envolvidas nas atividades vinculadas o Grupo Globalservice. É um documento interno, com valor jurídico e aplicabilidade imediata e indistinta a todos os seus colaboradores e parceiros que venham a ter acesso a dados pessoais e/ou recursos tecnológicos da organização.

## 3. DOCUMENTOS DE REFERÊNCIA

A presente política foi elaborada com base nas normas, leis e resoluções abaixo.

- ABNT NBR ISO/IEC 27000 e 27001 – Norma base para implantação de um Sistema de Gestão de Segurança da Informação – SGSI;
- Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018);
- Resolução nº 4.893/2021 do Banco Central do Brasil – Dispõe sobre a política de segurança cibernética;
- Código de Condutas Éticas; e
- Política de Vulnerabilidades.

## 4. OBJETIVOS

Esta política tem por objetivo estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores e parceiros do Grupo Globalservice adotar padrões de comportamento seguro, adequados às metas e necessidades da organização.

4.1. Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;
4.2. Resguardar as informações do Grupo Globalservice, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;
4.3. Prevenir possíveis causas de incidentes e responsabilidades legal da organização e seus colaboradores, clientes, terceirizados e parceiros; e
4.4. Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio do Grupo Globalservice como resultado de falhas de segurança.
4.5. Os riscos típicos que a aplicação desta Política pretende evitar são:

- Revelação de informações sensíveis;
- Revelação de informações pessoais;
- Modificações indevidas de dados e sistemas;
- Perda de dados e sistemas;
- Destruição ou interrupções de serviços essenciais;
- Roubo/furto de propriedade;
- Utilização indevida das informações; e
- Acessos não autorizados.

## 5. TERMINOLOGIA BÁSICA DA SEGURANÇA DA INFORMAÇÃO

**Confidencialidade** – a informação só deve ser acessível a quem tem a devida autorização;

**Integridade** – a informação deve manter-se inalterada desde sua geração ou alteração autorizada;

**Disponibilidade** – a informação deve estar sempre disponível às pessoas autorizadas;

**Informação** – resultado da produção, manipulação, organização ou processamento de dados que represente uma modificação no conhecimento do sistema que a recebe.

## 6. DIRETRIZES

O objetivo da Gestão de Segurança da Informação do Grupo Globalservice é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte as operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos a organização.

A Diretoria e o Comitê de Gestão da Segurança da Informação estão comprometidos com uma gestão efetiva de Segurança da Informação no Grupo Globalservice. Desta forma, adotam todas as medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da

organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às boas práticas e legislações vigentes.

## 7. SEGURANÇA DA INFORMAÇÃO

Nos tópicos a seguir serão definidas normas, procedimentos e boas práticas de segurança da informação no Grupo Globalservice.

### 7.1. Regras de Segurança da Informação

7.1.1. Toda e qualquer ação à informação no Grupo Globalservice deve ser orientada explicitamente por esta Política, resguardados os direitos e penalidades conforme legislação vigente.

7.1.2. O Grupo Globalservice reserva-se o direito de consultar e analisar informações armazenadas em suas dependências e em seus equipamentos, bem como em arquivos físicos e eletrônicos, geradas ou recebidas com utilização de seus recursos humanos e materiais.

7.1.3. Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação da empresa sejam atingidos através da adoção de controles contra ameaças provenientes de fontes externas quanto internas.

7.1.4. Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: colaboradores, terceiros contratados e, onde pertinente, clientes.

7.1.5. Garantir a educação e conscientização sobre as práticas adotadas pelo Grupo Globalservice de segurança da informação para colaboradores, terceiros contratados e, onde pertinente, clientes.

7.1.6. Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais.

7.1.7. Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade.

7.1.8. Tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas.

7.1.9. Melhorar continuamente o SGSI através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

7.1.10. A geração, utilização, armazenamento, manutenção, distribuição e destruição da informação devem ser feitas de acordo com as necessidades da empresa, sendo que estes processos devem estar devidamente documentados.

7.1.11. É obrigatória a cláusula de confidencialidade em todos os contratos de trabalho para que possa ser concedido o acesso do usuário aos ativos da informação disponibilizados pelo Grupo Globalservice.

7.1.12. Todos os equipamentos do Grupo Globalservice são de uso exclusivo para o alcance dos objetivos da organização e disponibilizados de acordo com as necessidades específicas dos usuários para o desempenho de suas atribuições.

7.1.13. A informação deve ser armazenada pelo tempo determinado na classificação da informação estabelecida pelo Grupo Globalservice ou legislação vigente, o que for maior, e recuperável quando necessário. O local de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos de pessoas não autorizadas.

7.1.14. Devem ser usados somente recursos autorizados para garantir o compartilhamento seguro da informação quando for necessário.

7.1.15. A informação sob custódia do Grupo Globalservice, mesmo que pertencente a clientes ou fornecedores, deve ser protegida contra o acesso de pessoas não autorizada.

### 7.2. Acesso à Informação

O uso de redes externas de comunicação (*Internet, redes privadas,* etc.) deve ser controlado através de Servidores de *Firewalls*, Servidores de Acesso à *Internet*, Servidores de *AntiSpam*, ferramentas de Antivírus e políticas de sistemas operacionais que garantam que somente os recursos necessários estejam disponíveis para o trabalho, sem riscos para o ambiente operacional.

7.2.1. O acesso externo aos sistemas da organização, quando realizado pelo pessoal da Área de Suporte Técnico ou por Prestadores de Serviço, deve ser controlado e restrito aos serviços necessários, mantendo trilhas de utilização e restringindo-se ao mínimo necessário. A solução encontrada para cada caso deve ser formalizada e documentada.

7.2.2. A remessa de dados da organização, seja para atender requisitos do negócio, como para viabilizar a resolução de problemas encontrados, deve ser avaliada em função dos riscos e pela adoção de procedimentos que garantam o controle e a integridade dos dados, além da legitimidade do receptor das informações. O que for acordado deve ser formalizado e aprovado pelos gestores responsáveis pela informação.

7.3. **Sistemas**

Sistemas desenvolvidos dentro da organização devem ser documentados e controlados quanto às alterações ou correções feitas, com trilhas do que foi feito e guarda segura da biblioteca de fontes. Toda informação necessária para eventual reconstrução dos aplicativos deve constar de sua documentação.

7.3.1. Sistemas desenvolvidos fora da organização, de propriedade de terceiros (com licença de uso para a organização), devem ter a biblioteca de fontes e de recursos adicionais (bibliotecas adquiridas, componentes, etc) sob custódia de uma entidade idônea, de comum acordo entre a organização e a empresa fornecedora do *software*. Tais fontes devem sempre ser atualizadas e verificadas quanto à sua validade e sincronização com a versão em uso no ambiente de produção.

7.3.2. O mau uso dos sistemas, feito de forma acidental ou deliberada, deve ser combatido pela segregação das funções de administração do sistema das funções de execução de certas atividades, ou entre áreas de responsabilidade. Tal segregação de funções visa criar controles para evitar fraudes ou conluios no desempenho de atividades críticas do sistema. Onde for impraticável implantar segregação, outros controles como monitoração das atividades, trilhas de auditoria e acompanhamento gerencial devem ser considerados.

7.3.3. Para minimizar o risco de falhas nos sistemas, deve-se fazer um planejamento e preparações prévias para garantir a disponibilidade e capacidade adequada dos recursos. Para novos sistemas os requisitos operacionais devem ser documentados e testados antes da sua aceitação e uso. Para sistemas já em uso devem ser feitas projeções da demanda de recursos e da carga da máquina futura a fim de reduzir o risco de indisponibilidade por sobrecarga.

7.4. **Tratamento da Informação**

7.4.1. Devem ser definidas regras claras para proteção da informação contra perda, alteração e acesso por pessoas não autorizadas, seja qual for o meio em que vier a ser armazenada (magnético, correspondências, relatórios, manuscritos etc).

7.4.2. Devem ser claramente definidos os usuários (empresas, áreas, pessoas etc) das informações, os direitos que cada um tem para acessá-las e os procedimentos para protegê-las do acesso por pessoas não-autorizadas, independentemente da forma como estiver disponível.

7.4.3. Toda informação deve ser utilizada apenas para fins profissionais, de interesse exclusivo da empresa.

7.4.4. Toda informação relevante deve ter pelo menos uma cópia reserva ou outro procedimento eficiente para pronta recuperação em caso de perda.

7.4.5. Nenhuma informação deve ser acessada, divulgada ou disponibilizada, sob qualquer pretexto, sem a devida autorização.

7.4.6. É proibida a transmissão a terceiros, por qualquer meio, bem como sua divulgação, reprodução, cópia, utilização ou exploração de conhecimentos, dados e informações de propriedade da organização, utilizáveis nas atividades das mesmas, sem a prévia e expressa autorização da Diretoria responsável, e das quais os funcionários venham a tomar conhecimento durante a relação empregatícia, estendendo-se tal vedação ao período após o término do contrato de trabalho, sem prejuízo das ações de natureza penal aplicáveis ao assunto.

7.4.7. Os usuários devem adotar a prática de classificação da informação com o objetivo de fornecer o tratamento adequado à informação nos aspectos de sua confidencialidade.

7.5. **Recomendações para o Tratamento da Informação**

7.5.1. A pessoa que receber indevidamente uma informação deve procurar imediatamente o remetente e alertá-lo sobre o equívoco.

7.5.2. As informações disponíveis na *Internet* somente deverão ser acessadas para fins de execução das atividades de interesse exclusivo da empresa.

7.5.3. Toda informação em papel, mídia removível ou qualquer outro meio de armazenamento somente poderá ser destruída se observado o prazo estabelecido na classificação da informação do Grupo Globalservice ou guardada de forma a não estar disponível para pessoas não autorizadas.

7.5.4. As manutenções em equipamentos que armazenem informações devem ser realizadas pela equipe de Tecnologia da Informação e acompanhadas por um representante da área sempre que esse equipamento estiver em uso ou logado com a credencial do colaborador que necessita o suporte. Quando forem vendidos, devolvidos ao fabricante, enviados para manutenção ou deslocados para outros usuários, as informações neles contidas deverão ser destruídas antes da liberação do equipamento.

7.5.5. Os gestores devem determinar as regras de acesso e distribuição das informações, considerando os seguintes itens:

**Riscos inerentes às informações:**

- Acesso por pessoas não autorizadas;
- Divulgação indevida;

- Indisponibilidade; e
- Alteração indevida.

**Consequências:**

- Fraudes: possibilidades de lesarem a organização ou terceiros (clientes, fornecedores, etc);
- Problemas legais: possibilidades de gerar prejuízos, multas, penalidades ou embaraços às instituições, Diretores, Funcionários do Grupo Globalservice, a outras pessoas físicas ou jurídicas;
- Perda do negócio: possibilidade não realizar receitas previstas ou gerar perdas nos negócios implantados ou em fase de implantação;
- Prejuízo da imagem da organização: possibilidades de prejudicar a imagem do Grupo Globalservice ou de seus funcionários; e
- Problemas de recuperação: possibilidades de gerar custos de recuperação de informações perdidas ou danificadas.

### 7.6. Segurança quanto às pessoas

Este tópico trata da segurança quanto às pessoas e tem como finalidade reduzir os riscos de erros humanos, roubo, fraude ou uso inadequado de informações e recursos do Grupo Globalservice.

7.6.1. Qualquer pessoa com acesso aos sistemas e informações do Grupo Globalservice, deverá ter uma única identificação (*login*). As exceções deverão ser devidamente documentadas e aprovadas pelo Comitê de Gestão da Segurança da Informação.

7.6.2. O Termo de Responsabilidade é um compromisso de responsabilidade direta do funcionário para com as informações, equipamentos e outras propriedades do Grupo Globalservice a ele confiadas, devendo ser lida e assinada quando da admissão de novos funcionários e a partir da implementação desta Política para os funcionários já contratados.

Este conceito deve ser utilizado também para prestadores de serviço e clientes:

7.6.3. **Prestadores de Serviço**: a declaração de responsabilidade deve ser uma das cláusulas do contrato. Em se tratando de contratos antigos, deve-se emitir o termo e solicitar ao responsável pela empresa sua ciência e assinatura.

7.6.4. **Clientes**: a declaração de responsabilidade deve ser uma das cláusulas do Contratação de Prestação de Serviços – ou documento equivalente, se ao cliente for entregue alguma senha de acesso às informações.

7.6.5. A declaração de responsabilidade deve ser lida e assinada por todos os funcionários antes de ser arquivada na respectiva pasta funcional. O Setor de Recursos Humanos deve garantir que todos os funcionários tenham sua declaração de responsabilidade assinada.

7.6.6. Poderá ser utilizado um Termo de Responsabilidade eletrônico, mediante aprovação do Comitê de Gestão da Segurança da Informação.

7.7. **Segurança de Computadores, Redes e Sistemas**

Todo sistema define um conjunto de operações aplicáveis as informações sob seu domínio. Tipicamente estas operações são: consulta, inclusão, alteração, exclusão, liberação etc.

7.7.1. Um perfil de acesso define que operações podem ser executadas por certa classe de usuários, usando um determinado tipo de informação.

7.7.2. As regras de acesso às informações de um sistema aplicativo devem incluir a definição dos perfis, permissões e classe de usuário, bem como os processos operacionais a serem utilizados para sua administração e controle.

7.7.3. Os acessos aos serviços e dados devem ser controlados com base nos requisitos de cada setor, devem estar claramente definidos e documentados e todos os sistemas devem estar direcionados para a implementação e manutenção desses controles.

7.7.4. A Gerência da TI juntamente com o Comitê da Informação devem definir e manter atualizada uma política de acesso aos sistemas.

## 8. ADMINISTRAÇÃO DO ACESSO AOS SISTEMAS

As informações devem ser analisadas pela Gerência de TI e Comitê de Gestão da Segurança da Informação, de forma a permitir que sejam definidas as regras de acesso, através de perfis e permissões. Os sistemas devem possuir recursos que possibilitem a administração dos acessos, através dos perfis e permissões definidos pelos respectivos gestores da informação.

8.1. **Administração do acesso de usuários:**

8.1.1. Devem existir procedimentos formais que contemplem todas as atividades ligadas à administração de acessos, desde a criação de um usuário novo, passando pela administração de privilégios e incluindo a desativação de usuários.

8.2. **Controle de acesso a computadores e redes:**

8.2.1. Deve ser assegurado que usuários de computadores, conectados ou não a uma rede, não comprometam a segurança de qualquer sistema ou produto.

8.2.2. O acesso a serviços computacionais deve ocorrer sempre através de um procedimento seguro, pelo qual o usuário conecta-se a um determinado sistema ou rede, que deve ser planejado para minimizar as oportunidades de acessos não autorizados.

8.2.3. A Tecnologia da Informação do Grupo Globalservice, deve tomar ações no sentido de impedir acessos indevidos.

8.3. **Monitoramento de uso e acesso aos sistemas:**

Todos os sistemas deverão:

a) Detectar tentativas de acesso não autorizado.
b) Registrar eventos de entrada no sistema (*login).*
c) Sempre que houver riscos que afetem o negócio devem ser gravadas trilhas de auditoria para futuras investigações, registrando os dados de acesso, tais como: identificação do usuário, localidade, identificação do terminal ou estação de rede, data e hora do acesso, identificação do aplicativo acessado e transações executadas.
d) Emitir relatórios gerenciais de acessos (por usuário, módulo do aplicativo e funções).

## 9. SEGURANÇA NO ACESSO DE PRESTADORES DE SERVIÇO

Deve ser feita uma avaliação dos riscos envolvidos para determinar as implicações de segurança e os controles necessários. O que for acordado deve ser explicitado no contrato assinado.

## 10. SEGURANÇA FÍSICA DE COMPUTADORES

O objetivo é garantir que os setores estabeleçam, administrem e utilizem computadores de maneira segura e que sejam tomadas ações adequadas para respeitar a confidencialidade, integridade e disponibilidade das informações que são armazenadas e manipuladas através destes equipamentos.

### 10.1 Normas para segurança física de computadores

10.1.1. Os meios de armazenamento considerados como mídias removíveis devem ter acesso controlado. Quando não estiverem sendo utilizados, devem ser trancados, com acesso restrito a pessoas autorizadas.

10.1.2. Os computadores não ligados a uma rede e que contenham informações importantes para os negócios da empresa, devem estar instalados em uma estrutura que garanta a segurança física destes equipamentos, incluindo sistemas que mantenham fornecimento de energia elétrica e recuperação de dados.

10.1.3. Os usuários ligados a uma rede, e que tratam com informações importantes para os negócios da empresa, devem manter estas informações armazenadas nos servidores de rede.

10.1.4. O setor de Tecnologia da Informação – TI do Grupo Globalservice é responsável por elaborar e manter atualizado o inventário de *hardware* e *software* da organização.

10.1.5. A Gerência de TI é responsável por garantir o controle sobre o acesso físico aos equipamentos.

## 11. PRECAUÇÕES QUANTO ÀS MÍDIAS DE ARMAZENAMENTO

Quando as mídias removíveis de armazenamento forem vendidas, devolvidas ao fabricante ou enviada para manutenção, as informações nelas contidas devem ser destruídas antes de deixar as dependências da organização. Importante ressaltar que nos meios magnéticos não é suficiente apagar os dados, devendo-se executar um programa que realmente os destruam.

11.1. O objetivo é garantir que a organização administre e utilize os diversos sistemas operacionais de maneira segura, e que sejam tomadas medidas adequadas para garantir a confidencialidade de seus dados, a integridade e disponibilidade dos equipamentos e meios de armazenamento.

11.2. A Gerência de TI do Grupo Globalservice é responsável por garantir o controle de acesso físico aos equipamentos.

## 12. COMITÊ DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO – CGSI

O Comitê foi instalado para tratar de assuntos referentes à segurança da informação, doravante denominado Comitê de Gestão da Segurança da Informação – CGSI. O referido comitê foi composto por um representante da Direção, Gerência de TI, Gerência de RH, Gerência Geral, Assessor Jurídico e a empresa Aguiar Soluções.

## 13. BACKUP

O responsável pela TI da organização criará as definições e executará os procedimentos e manuais operacionais específicos, conforme as características das informações, dos sistemas e das ferramentas de geração de backup, devendo considerar as seguintes diretrizes:

13.1. O armazenamento seguro e ambientalmente adequado em instalações locais e remotas das mídias, incluindo a eventual geração de backups redundantes como suporte às estratégias de contingência operacional e de continuidade de negócios.

13.2. Utilização de criptografia e restrição de acesso ao material salvaguardado.

13.3. O descarte seguro de mídias e ferramentas de geração de backups obsoletos, depreciação e danificados, considerando a eliminação definitiva de seu conteúdo e, quando necessário, a destruição do suporte físico.

## 14. UTILIZAÇÃO SEGURA DE *HARDWARE* E *SOFTWARE*

Todos os equipamentos portáteis (*notebooks, laptops, netbooks, ultrabooks, tablets e smartphones*) que tenham capacidade de armazenamento de dados, devem ser protegidos conforme especificação da empresa. Quando estes equipamentos

contiverem informações que não possam ser de conhecimento público, as mesmas devem ser criptografadas ou ter seu acesso protegido por senha.

14.1. É proibida a utilização de qualquer equipamento particular nas dependências da empresa, exceto telefones corporativos fornecidos para otimizar a comunicação interna.

14.2. É expressamente vedada a aquisição, reprodução, utilização e cessão de cópias não autorizadas de "*softwares*" ou de quaisquer programas e produtos.

## 15. SERVIÇOS PORTAL DE CHAMADOS

É responsabilidade de todo usuário da informação do Grupo Globalservice informar incidentes de segurança da informação e/ou solicitar serviços, somente através do Portal de Chamados.

Ao acessar a rede corporativa através de login e senha, o usuário terá à sua disposição os seguintes serviços:

15.1. Abertura de chamados, podendo ser: incidente ou requisição;

15.2. Acompanhamento do chamado realizado;

15.3. Realizar reserva de dispositivos ou equipamentos da TI e;

15.4. Utilizar a opção Perguntas Frequentes (FAQ) e tirar dúvidas básicas.

## 16. ACESSO À INTERNET

A *Internet* abrange vários aspectos e serviços (*websites* de serviços governamentais, prestadores de serviço e outros) que devem ser disponibilizados de forma restrita ou controlados conforme as necessidades do negócio. A restrição a *websites* não relativos aos negócios da empresa deve ser implementada, garantindo o uso efetivo da rede.

16.1. O acesso à Internet deve ser rastreado a fim de permitir o monitoramento do uso indevido da tecnologia (nome do usuário e endereço acessado são informações obrigatórias no rastreamento).

16.2. O usuário deve restringir o acesso aos *websites* ainda não bloqueados que possam denegrir a imagem da organização (por exemplo: pornografia, pedofilia, racismo etc.) e que não tem relação com os objetivos de negócio da organização (*webmail*, jogos etc.).

16.3. Deve também comunicar o endereço eletrônico desses *websites* à Gerência de TI, que deverá realizar seu imediato bloqueio.

## 17. ACESSO AO CORREIO ELETRÔNICO

O Grupo Globalservice disponibiliza aos seus funcionários a tecnologia necessária a fim de facilitar a comunicação interna, comunicação com clientes, fornecedores e outros grupos que tenham relação comercial com a mesma. É de responsabilidade do usuário a utilização da tecnologia de forma adequada, prudente, e de modo compatível com as leis e princípios aplicáveis aos negócios.

As mensagens de correio eletrônico devem ser rastreadas, a fim de permitir o monitoramento para identificar o uso indevido da tecnologia.

## 18. PLANO DE CONTINUIDADE DO NEGÓCIO

Um Plano de Continuidade do Negócio deve garantir a recuperação dos processos críticos da organização quando da indisponibilidade do ambiente ou de quaisquer recursos que impossibilitem o desenvolvimento ou as operações das áreas de negócio.

A definição de processos críticos da empresa, obrigatoriamente, deve obedecer a critérios emanados pelo Gestor responsável do setor.

Na elaboração de um plano de continuidade de negócio os pontos abaixo devem ser observados:

a. As funções críticas devem ser identificadas e definidas.
b. Traçar uma estratégia para recuperação de cada função crítica.
c. Priorizar as funções críticas para ordenar sua recuperação.
d. Identificar as atividades necessárias para recuperar cada função.
e. Quantificar os recursos humanos e técnicos necessários ao cumprimento do plano.
f. Documentar os processos críticos.
g. Identificar os responsáveis pela recuperação de cada processo ou função.
h. Ações para restabelecer a operação normal.
i. Identificar os recursos de *backup* (infraestrutura, *hardware*, *software,* sistemas aplicativos e telecomunicação).

O plano de continuidade do negócio deverá sofrer revisões periódicas a fim de identificar pontos que estiverem em desacordo com a situação atual. Deverão ser observados os pontos abaixo:

a) Troca de fornecedores ou contratados;
b) Alteração de endereços ou números de telefone;
c) Mudanças nas prioridades de recuperação;
d) Interdependência entre sistemas e aplicativos;
e) Mudanças nas funções e nos processos críticos do negócio; e
f) Mudanças nas práticas operacionais.

## 19. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Os incidentes de Segurança da Informação serão prevenidos:

19.1. Pela fiscalização do cumprimento da legislação vigente no Brasil, dos princípios éticos e dos controles estabelecidos pelos normativos do Grupo Globalservice.

19.2. Pelo monitoramento das vulnerabilidades existentes por meio de ferramentas de supervisão de atividades, registro e análise de trilhas de auditoria e controle de acesso em ambientes físicos e digitais.

19.3. O colaborador ou parceiro deve relatar todos os incidentes de segurança da informação que tiver conhecimento imediatamente ao Gestor da Área e à Gerência de Tecnologia da Informação do Grupo Globalservice.

19.4. O colaborador não deve tomar qualquer ação própria em busca da solução do incidente de segurança da informação, devendo apenas relatá-lo.

19.5. Os índices de segurança da informação são quantificados e monitorados pelo setor de Tecnologia da Informação do Grupo Globalservice, a fim de identificar quais podem ser mais recorrentes ou de maior impacto, além de permitir implementar ações corretivas e prevenir novas ocorrências.

19.6. Após notificação de um incidente de segurança da informação, a Gerência da Tecnologia da Informação e o Comitê de Gestão da Segurança da Informação devem tomar as ações necessárias para a mitigação de seus impactos e o restabelecimento da condição de normalidade.

19.7. As ações visam garantir a proteção aos direitos do titular de dados, a continuidade dos negócios do Grupo Globalservice e de suas atividades, além de realizar o isolamento do ambiente e do dispositivo, caso seja necessário.

19.8. Sempre que ocorrerem indícios do envolvimento de um colaborador ou parceiros em um incidente de segurança da informação, a Gerência de TI deve realizar o bloqueio de sua identidade digital e demais acessos, além de informar imediatamente o Gestor da Área.

19.9. É de responsabilidade da empresa Aguiar Soluções e da Gerência de TI da organização elaborar e publicar o Plano de Resposta a Incidentes Cibernéticos, esse plano deve conter cada etapa de cada tratativa a partir da identificação de um incidente. Seu objetivo é criar uma abordagem e conduta, minimamente necessária, em caso de um incidente cibernético na organização.

## 20. IMPRESSÃO

O serviço de impressão destina-se exclusivamente as atividades de cunho empresarial da organização. A sustentabilidade ambiental é elemento chave na utilização do serviço – a impressão de documentos deve ser evitada sempre que possível.

20.1. Deve-se buscar a tramitação de processos administrativos da empresa sempre na forma eletrônica, fazendo uso da impressão apenas nos casos em que se requer assinatura ou carimbos impressos ou que seja um pré-requisito.

20.2. Quando usado a impressão deve ser impressa em dupla-face sempre que possível. Evitar a impressão de qualquer dado pessoal conforme elencado na Lei nº 13.709/2018 LGPD.

20.3. Ao imprimir qualquer documento o colaborador deverá adotar todos os cuidados de segurança necessários para que nenhuma pessoa sem autorização tenha acesso a dados confidenciais e/ou pessoais de qualquer cliente, colaborador, fornecedor e/ou prestador de serviço do Grupo Globalservice. Qualquer impresso que já cumpriu sua necessidade deve ser desfragmentado.

## 21. MESA LIMPA

O Grupo Globalservice adota as seguintes ações para minimizar os riscos associados ao acesso indevido, perda ou destruição de informações durante e fora do seu expediente:

21.1. Manter a sua mesa organizada.

21.2. Ao se ausentar da mesa, guardar qualquer documento que possa conter dados pessoais ou estratégicos da organização e de seus clientes.

21.3. Não deixar exposto informações estratégicas, dados pessoais e senhas em postites ou papeis colados em sua mesa.

21.4. No final do expediente, recolher papéis e documentos da sua mesa, eliminando aqueles que não possuem mais uso.

## 22. CLASSIFICAÇÃO DA INFORMAÇÃO

Todos os usuários são responsáveis pelas informações do Grupo Globalservice que circulam em diferentes formatos e meios de comunicação, dentro e fora da organização.

22.1. Toda informação deve ser protegida e mantida sob sigilo conforme a sua importância e criticidade para o Grupo Globalservice.

22.2. Quanto mais crítica ou sigilosa, maiores cuidados devem ser delicados ao manuseio, arquivamento e eventual descarte.

22.3. O Grupo Globalservice trabalha com documentos físicos e eletrônicos criados internamente ou recebidos de terceiros. Todos os documentos são de propriedade da organização e, portanto, devem ser protegidos, pois podem conter informações corporativas críticas.

22.4. O Comitê de Gestão da Segurança da Informação é responsável pela classificação dos tipos de documentos.

22.5. O processo de classificação da informação consiste em identificar quais são os níveis de proteção requeridos, bem como estabelecer classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas. O sistema de classificação de informação do Grupo Globalservice obedece a seguinte estrutura de acordo com a sua criticidade.

22.6. **Informação Confidencial** – é a informação da organização e/ou de seus clientes e parceiros com o mais alto grau de confidencialidade e restrição e que, se for divulgada sem autorização, pode causar danos materiais significativos ou até mesmo colocar em risco a viabilidade do negócio. São limitadas a um número reduzido de pessoas, pois exigem medidas especiais de controle e proteção contra acessos ou cópias não autorizadas.

22.7. **Informação Interna** – é toda informação cujo conhecimento é limitado ao ambiente interno e aos propósitos da organização. Apenas os colaboradores, estagiários ou aprendizes e prestadores de serviços podem ter acesso a essas informações e sua revelação ao público em geral só poderá ocorrer se explicitamente autorizada pelo Grupo Globalservice.

22.8. **Informação Pública** – é a informação para uso interno e/ou externo com controles mínimos cuja divulgação pública não causa impacto ao Grupo Globalservice. É colocada à disposição do colaborador ou prestador de serviço e pode ser revelada ao público externo.

22.9. **Informação não Classificada** – toda informação não classificada deve ser considerada como INTERNA.

## 23. GESTÃO DA IDENTIDADE

A identidade digital concedida ao colaborador é composta por um identificador único (ID ou nome do colaborador) e por um mecanismo de autenticação sigiloso (senha, biometria, token).

23.1. O responsável pela Tecnologia da Informação irá configurar o primeiro acesso do colaborador atribuindo uma senha temporária de modo que seja obrigatória sua alteração em seguida autenticação.

23.2. A senha deve ser tratada de forma individual, sigilosa e intransferível, não podendo ser compartilhada ou divulgada a terceiros. A senha não deve ser armazenada nos computadores ou dispositivos móveis, anotadas em papel ou em qualquer outro suporte físico ou eletrônico.

23.3. As senhas dos colaboradores devem:

a) Conter, pelo menos 15 (quinze) caracteres, dentre letras maiúsculas e minúsculas, números e símbolos.

b) 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.

c) Não devem ser constituídas de combinações óbvias de teclado, como "abcdefg", "87654321", entre outras.

d) Serem trocadas em até 35 (trinta e cinco) dias.

e) Não serem idênticas às últimas 10 (dez) utilizadas.

f) Os colaboradores devem ter autenticação 2FA e a mesma deve ser habilitada.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 20 (vinte) caracteres, dentre letras maiúsculas e minúsculas, números e símbolos.

a) Sempre que houver suporte à autenticação multifator MFA a mesma deve ser habilitada.

b) Serem trocadas entre 60 (sessenta) e 90 (noventa) dias.

c) Não serem idênticas às últimas 10 (dez) utilizadas.

d) Ser alteradas em qualquer caso de suspeita do comprometimento de seu sigilo ou vazamento.

## 24. ARMAZENAMENTO E DESCARTE DE INFORMAÇÕES FÍSICAS

O Grupo Globalservice deve cumprir os diferentes prazos que a legislação estabelece para manutenção e guarda de documentos e livros fiscais, físicos e digitais, de acordo com a área correlata ao conteúdo das informações, a exemplo, mas não se limitando a documentos societários, tributários, trabalhistas e previdenciários.

24.1. Não é permitido o descarte em lixo comum de documentos confidenciais, como notas fiscais, balanço, extratos bancários, impressões de qualquer espécie ou tipo. Os documentos desta natureza devem ser triturados em seu descarte físico.

24.2. A guarda de documentos deve ser organizada, sigilosa, segura e com movimentação restrita a colaboradores previamente autorizados.

## 25. TREINAMENTO

O Grupo Globalservice preza pela excelência da execução de suas atividades, sendo a segurança e proteção de dados uma delas, desta forma ela se compromete que seus colaboradores e parceiros passem por treinamento adequados e periódicos em boas práticas de segurança da informação. Desta maneira fica determinada nesta política:

25.1. Treinamento anual de LGPD e Resolução nº 4893 do Bacen ou sempre que houver atualização de ambas.

25.2. Treinamento LGPD e Resolução nº 4893 do Bacen na integração de novos colaboradores e parceiros e aos colaboradores veteranos e parceiros veteranos por ocasião da implantação do SGSI.

25.3. Estes treinamentos são adotados como obrigatórios dentro da empresa, sempre serão ministrados por empresas ou profissionais capacitados sobre o assunto.

## 26. IDENTIFICAÇÃO VISUAL

O uso do crachá de identificação do Grupo Globalservice é obrigatório, pessoal e intransferível para todos os colaboradores. Deverá ser portado em lugar bem visível durante todo o tempo de permanência na empresa. Quando executar serviços externos, o colaborador também deverá usá-lo nas mesmas condições quando visitar clientes. O uso do crachá é imprescindível para segurança do ambiente de trabalho.

26.1. Em caso de perda ou extravio o funcionário ou parceiro deve comunicar de imediato a ocorrência ao Gestor Imediato e este à Gerência de RH, formalmente.

26.2. Um novo crachá deve ser solicitado imediatamente ao Setor de RH.

## 27. CERTIFICADO DIGITAL

O único certificado digital a ser utilizado para execução das atividades laborais é o certificado e-CNPJ tipo A1 do Grupo Globalservice.

27.1. É vedado ao colaborador confiar a guarda ou compartilhar o certificado digital da organização a terceiros, ou utilizar certificados digitais de terceiros sem a devida procuração.

27.2. É terminantemente proibido ao colaborador utilizar certificado digital de empresas clientes, seja qual for a mídia (cartão, pen-drive, arquivo) ou nível de segurança (A1, A2, A3, A4).

27.3. É vedado ao colaborador utilizar seu certificado e-CPF, caso possua, para realizar trabalhos profissionais. Tal certificado deve ser mantido em sua posse.

27.4. Caso alguma das atividades exija a utilização do certificado digital dos sócios e que não seja possível a utilização de procuração (por ex. e-CPF para entrega de declarações) o uso destes, está condicionado a autorização por escrito do respectivo sócio, conforme Termo de Autorização.

27.5. Os dispositivos de identificação e senhas, incluindo os certificados digitais, protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra pessoa perante o Grupo Globalservice e/ou terceiros. Por isso, o uso dos dispositivos, incluindo certificados digitais e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

27.6. Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

## 28. MONITORAÇÃO E INSPEÇÃO

Os colaboradores e prestadores estão cientes de que o Grupo Globalservice realiza o registro e armazenamento de atividades (logs), e monitora todo acesso e uso de seus ambientes físicos e digitais com a captura de imagens, áudio ou vídeo, inclusive, com a finalidade de proteção de seu patrimônio e reputação e daqueles com quem se relaciona, de alguma forma, além de colaborar com as autoridades em caso de investigação.

28.1. Sempre que julgar necessário, o Grupo Globalservice pode auditar ou inspecionar os recursos de tecnologia que interagem com seus ambientes físicos ou digitais ou com suas informações, quando autorizada a entrada em suas dependências.

## 29. LGPD

A LGPD foi promulgada em 2018 com o objetivo de trazer ao ordenamento jurídico brasileiro uma preocupação que já tem lugar em todos os países desenvolvidos: a proteção de dados pessoais. No mundo todo, a legislação de proteção a dados de pessoas naturais é um instrumento necessário para garantir maior segurança jurídica e respeitabilidade aos direitos humanos fundamentais. Assim sendo, a conformidade com tais leis tem sido um fator importante para o Grupo Globalservice.

São princípios norteadores da Lei Geral de Proteção de Dados e também os desta política interna:

**Adequação**: o tratamento dos dados tem que ser compatível com a finalidade informada ao titular.

**Necessidade**: o tratamento deve ser limitado ao mínimo necessário para atingir a finalidade proposta.

**Livre acesso**: os titulares têm o direito de acessar a qualquer tempo as informações referentes ao tratamento que seus dados recebem.

**Qualidade dos dados**: o tratamento dos dados deve mantê-los exatos, claros, relevantes e atualizados, sem discrepâncias ou distorções.

**Transparência**: o tratamento dos dados deve ser explicado aos titulares de maneira transparente e acessível, observado o segredo comercial e industrial necessário.

**Segurança**: os dados pessoais devem ser protegidos pelo controlador, para que não sejam perdidos, alterados, destruídos ou acessados indevidamente.

**Prevenção**: cabe ao controlador tomar medidas para prevenir danos provenientes do tratamento de dados pessoais.

**Não discriminação**: o tratamento de dados pessoais não deve ser realizado com finalidades discriminatórias, ilícitas ou abusivas.

**Responsabilização e prestação de contas**: demonstração, aos titulares, das medidas utilizadas para garantir conformidade com a Lei Geral de Proteção de Dados Pessoais.

## 30. VEDAÇÕES

Quando da utilização dos recursos tecnológicos do Grupo Globalservice, o colaborador ou parceiro não deve:

a. Realizar qualquer tipo de manutenção ou reparo nos recursos tecnológicos corporativos, exceto o responsável de TI ou terceiro autorizado pelo Grupo Globalservice.

b. Utilizar programas que burlem os controles de segurança e controle impostos pelo Grupo Globalservice ou por seus normativos.

c. Executar programas de compartilhamento de arquivos ou estrutura diversa que permita a interconexão entre usuários de diversas localidades por meio de redes públicas, exceto quando prévia e expressamente autorizado.

d. Acesso a sites que realizem o redirecionamento de tráfego (proxy) e burlem as políticas digitais.

e. Desinstalar ou desabilitar softwares instalados nos recursos tecnológicos pelo Grupo Globalservice ou por alguém à sua ordem, independentemente do motivo.

f. Acessar informações confidenciais sem explícita autorização do responsável.

g. Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes.

h. Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

i. Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autoriais de propriedades intelectuais sem a devida autorização legal do titular.

j. Hospedar, acessar e compartilhar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país.

k. Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

l. Realizar transferência e/ou a divulgação de qualquer software, programa ou dados para terceiros, por qualquer meio de comunicação (físico ou digital), 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.

m. Armazenar arquivos pessoais e/ou não pertinentes ao negócio do Grupo Globalservice (fotos, músicas, vídeos etc.), para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores e acumular dados não necessários as atividades do Grupo Globalservice. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente, facultando a empresa em comunicar previamente o usuário.

n. O consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

o. A utilização de dispositivos removíveis de armazenamento de informações (pen drives, CDs, DVDs, HD Externos) para o transporte de informações. Em extremas necessidades e exceções é necessário acionar o responsável da TI para a avaliação do caso junto ao gestor responsável, se permitido, o dispositivo deverá conter tecnologia de criptografia. Todo o conteúdo transporte deve ser armazenado na rede corporativa e apagado do dispositivo imediatamente após a utilização.

p. O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato).

q. O acesso, armazenamento, utilização ou compartilhamento a conteúdo agressivo, ofensivo, difamatório, ridicularizante, calunioso, constrangedor, violento, abusivo, homofóbico, racista ou político.

r. Que represente uma quebra de confidencialidade das informações do Grupo Globalservice ou de seus clientes.

s. Caracterize assédio moral ou sexual, ou que incitem a prática de crimes ou contravenções penais.

t. Constitua violação aos direitos de propriedade intelectual ou industrial do Grupo Globalservice, a exemplo dos bancos de dados, segredos de negócio, dados contábeis ou financeiros, ou de terceiros, incluindo a proteção de suas marcas e patentes.

u. Que denote ou estimule a perseguição preconceituosa baseada em cor, sexo, raça, incapacidade física ou mensal, condição social, origem, religião, orientação sexual ou outras situações protegidas em leis brasileiras.

## 31. PAPÉIS E RESPONSABILIDADES

Abaixo serão elencadas as responsabilidades dos envolvidos na Política de Segurança da Informação do Grupo Globalservice.

**Diretores, sócios e gestores**

a) Aprovar os normativos da organização.
b) Orientar e acompanhar o estabelecimento e a observância dos controles estabelecidos, além de analisar as questões específicas apresentadas pelos colaboradores da organização.

**Gerência de TI**

a) Definir com as demais áreas da organização os requisitos e controles adequados para a proteção das informações e recursos tecnológicos da mesma.
b) Avaliar periodicamente os sistemas e equipamentos, com o intuito de verificar o cumprimento dos normativos da empresa.
c) Implementar os controles de segurança previstos nesta Política para proteção das informações e dos recursos tecnológicos.
d) Manter os *softwares* de proteção instalados, ativos e atualizados.
e) Adquirir, de acordo com o orçamento da organização, recursos tecnológicos necessários a proteção da informação, quando autorizado pela Diretoria.
f) Tomar as ações cabíveis em caso de perda, furto ou roubo de qualquer recurso tecnológica da organização.

g) Proceder com a manutenção, instalação, análise, configuração ou remanejamento de quaisquer recursos tecnológicos da empresa.
h) Estabelecer mecanismos de identificação e autenticação de forma que possibilite a rastreabilidade das atividades do colaborador ou parceiro.
i) Auxiliar no processo de revisão de acessos concedidos.
j) Fornecer a senha ao colaborador ou parceiro de forma segura, sigilosa e de maneira que a sua alteração seja exigida no primeiro acesso.
k) Conceder, ajustar ou revogar o acesso do colaborador ou parceiro, quando solicitado formalmente ou em caso de demissão ou encerramento das atividades.
l) Realizar e testar o backup das informações e recursos tecnológicos críticos para a organização.
m) Realizar o monitoramento e manter o valor probatório dos registros para fins legais, preservando a confidencialidade, integridade, autenticidade, legalidade e disponibilidade das informações.

**Gerência de RH**

a) Auxiliar na promoção da divulgação e capacitação sobre segurança da informação na empresa.
b) Comunicar formal e imediatamente qualquer admissão, alteração de cargo ou de atividade e demissão para a Gerência de TI, para que este crie, altere ou cancele as contas de acesso correspondentes.
c) Informar o encerramento das atividades, férias, licenças, ausência temporária dos colaboradores à Gerência de TI, imediatamente.

**Empresa Aguiar Soluções**

a) Conduzir a Gestão e Operação da Segurança da Informação, tendo como base esta política e demais resoluções do CGSI.
b) Apoiar o CGSI em suas deliberações.
c) Elaborar e propor ao CGSI as políticas, normas e procedimentos de segurança da informação, necessários para se fazer cumprir esta política.
d) Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco.
e) Tomar as ações cabíveis para se fazer cumprir os termos desta política.
f) Em parceria com o CGSI realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.
g) Auxiliar na divulgação e capacitação dos colaboradores e demais parceiros sobre segurança da informação no Grupo Globalservice.
h) Realizar os treinamentos de segurança da informação e proteção de dados, conforme periodicidade estabelecida nesta norma.
i) Elaborar e manter atualizada as políticas, normas e procedimentos de segurança da informação e proteção de dados.
j) Orientar constantemente todos os setores quanto ao uso ético, seguro e de acordo com a legislação nacional vigente dos ativos tangíveis e intangíveis do Grupo Globalservice.

k) Participar da investigação de incidentes de segurança relacionados às informações e Recursos da TI.
l) Realizar reuniões, Diálogo Semanal de Segurança da Informação e demais ações necessárias para orientação e conscientização de todos.

**Gestor do Colaborador / Parceiro**

a) Orientar constantemente suas equipes quanto ao uso ético, seguro e de acordo com a legislação nacional vigente dos ativos tangíveis e intangíveis da empresa.
b) Autorizar ou não, o uso de dispositivos móveis corporativos pelos colaboradores supervisionados.
c) Assegurar o cumprimento desta Política por parte dos colaboradores supervisionados.
d) Participar da investigação de incidentes de segurança relacionados às informações, recursos tecnológicos e colaboradores sob sua responsabilidade.

**Colaboradores e Parceiros**

a) Cumprir e manter-se atualizado em relação a esta Política.
b) Utilizar de forma ética, segura e de acordo com a legislação nacional vigente todos os ativos corporativos, respeitando os direitos e as permissões de uso concedidas pela organização.
c) Zelar para que todas as informações inseridas nos recursos tecnológicos da empresa, ou quando enviadas ao cliente, sejam necessárias, livres de erro, transparentes e verídicas.
d) Utilizar as informações e os recursos tecnológicos da organização somente para finalidades profissionais e restritas as atividades contratadas.
e) Classificar e rotular todas as informações confidenciais no momento da sua criação ou recebimento.
f) Tratar a senha de forma individual, sigilosa e intransferível, não compartilhando ou divulgando a terceiros.
g) Triturar as informações físicas, sempre que necessário seu descarte.
h) Reportar imediata e formalmente qualquer caso comprovado, passível de comprovação ou cuja suspeita seja fundamentada de descumprimento desta Política ou de qualquer incidente de segurança da informação, sob pena de sua conduta ser considerada omissa, negligente ou conivente.
i) Atuar de forma transparente, imparcial, evitando toda forma de privilégios, benefícios, corrupção, fraude, suborno, favorecimento, extorsão e vantagens.

**Comitê de Gestão da Segurança da Informação – CGSI**

a) Aprovar e revisar anualmente, ou sempre que se faça necessário, esta Política e os demais processos e procedimentos que envolvem a segurança da informação e o processo de gerenciamento de incidentes de segurança da informação em harmonia com as diretrizes nacionais.
b) Estabelecer um Programa de Gestão de Riscos, atualizando-o quando necessário.
c) Analisar e Aprovar todas as Políticas, Planos e Procedimentos desenvolvidos pela Aguiar Soluções.

d) Analisar e Aprovar todos os mecanismos de registro e controle de não conformidade a esta Política, desenvolvidos pela Aguiar Soluções.
e) Recepcionar, analisar e tratar toda e qualquer reclamação, comunicação e solicitação, por qualquer meio de entrada.

## 32. SANÇÕES E PUNIÇÕES

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa;

31.1. A aplicação de sanções e punições será realizada conforme a análise do Comitê de Condutas Éticas – COMCE, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho – CLT, podendo o CGSI, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave;

31.2. No caso de terceiros contratados ou prestadores de serviço, o CGSI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato;

31.3. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano o Grupo Globalservice, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens.

31.4. O colaborador que tomar atitudes antiéticas, ilícitas, não autorizadas ou contrárias ao recomendado pelo Grupo Globalservice devem ser consideradas violações por si só e estão sujeitas às sanções cabíveis, podendo variar desde advertência verbal ou escrita, até a rescisão do contrato de trabalho.

31.5. A tentativa de burlar às diretrizes e controles estabelecidos pelo Grupo Globalservice deve ser desestimulada e, quando constatada, será tratada como violação às normas da empresa.

## 33. CASOS OMISSOS

Os casos omissos serão avaliados pelo Comitê de Condutas Éticas – COMCE para posterior deliberação.

## 34. DISPOSIÇÕES FINAIS

Esta política encontra-se disponível em todos os canais de comunicação do grupo, juntamente com o Termo de Responsabilidade, para fins de ciência.

Em caso de dúvidas, o colaborador ou parceiro pode solicitar os esclarecimentos necessários para o e-mail: sgsi@globalservice-am.com.br.

## 35. DISPOSIÇÕES GERAIS

O Grupo Globalservice é composto pelas seguintes empresas:

- Globalservice Segurança Eletrônica Ltda
  Segmento de Atuação: Segurança Eletrônica
  CNPJ nº 05.667.700/0001-58

- Globalservice Serviços Empresariais Ltda
  Segmento de Atuação: Serviços de Portaria, Conservação e Limpeza
  CNPJ nº 07.989.755/0001-00

- Globalservice Vigilância e Segurança Ltda
  Segmento de Atuação: Vigilância Armada e Desarmada
  CNPJ nº 84.526.045/0001-94

- Globalservice Transportes de Valores Ltda (Matriz)
  Sede da Empresa: Manaus/AM
  Segmento de Atuação: Transporte e Custódia de Valores
  CNPJ nº 07.782.730/0001-30 (Matriz)

- Globalservice Transporte de Valores Ltda (Filial)
  Sede da Empresa: Rio Branco/AC
  Segmento de Atuação: Transporte e Custódia de Valores
  CNPJ nº: 07.782.730/0002-11

## 36. REVISÕES

Esta política será revisada com periodicidade anual ou conforme o entendimento do Comitê de Gestão da Segurança da Informação – CGSI.

## 37. GESTÃO DA POLÍTICA

A revisão 1.2 da Política de Segurança da Informação foi aprovada pelo Comitê de Gestão da Segurança da Informação – CGSI e pela Diretoria do Grupo Globalservice.

Manaus/AM, 18 de novembro de 2024.

**Alcimar Leão de Oliveira**
Diretor Administrativo e Financeiro

**Érika Aguiar de Souza**
Comitê de Gestão de Segurança da Informação