1. INTRODUÇÃO E OBJETIVOS

Esta Política de Segurança da Informação (PSI) está em consonância com a legislação vigente do país e baseia-se nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2022, reconhecida mundialmente como um Código de Boas Práticas para a Gestão da Segurança da Informação. Diante disso, a Golden Cloud Technology decide implantar um Sistema de Gestão Integrado (SGI), cuja estrutura e diretrizes de Segurança de Informação são expressas neste documento.

A Golden Cloud Technology, em razão de seu compromisso com a proteção das informações de sua propriedade, estabelece diretrizes para proteção dos ativos de informação e níveis aceitáveis de confiabilidade, devendo ser observadas por todos os seus colaboradores.

De modo geral, esta Política resume os princípios de Segurança da Informação que a Golden Cloud Technology reconhece como sendo importantes, devendo estar presentes no cotidiano de suas atividades. Assim, visa assegurar a confidencialidade, disponibilidade e integridade do processamento, transferência, manuseio e armazenamento das informações críticas que estão no escopo do SGI.

A Política de Segurança da Informação também demonstra o comprometimento de seguir os objetivos de Segurança de Informação descritos no Plano do Sistema de Gestão Integrado. A fim de garantir a adequação contínua, esta Política será atualizada anualmente.

Todos os funcionários, estagiários e prestadores de serviço que tenham qualquer envolvimento com os ativos e informações críticas coberto pelo escopo do SGI são responsáveis por seguir as políticas, diretrizes, normas, planos, processos e procedimentos de gestão da Golden Cloud Technology.

2. ESCOPO E ABRANGÊNCIA

A Política de Segurança da Informação e o Plano do Sistema de Gestão Integrado formam a base para o estabelecimento dos padrões e procedimentos de segurança da Golden Cloud Technology, abrangendo todos os seus sistemas e ambientes de Tecnologia da Informação.

É destinada a todos os seus funcionários, estagiários e prestadores de serviço, que atuam sob contrato, e que, no desenvolvimento de suas atribuições, fazem uso de informações de negócio ou administrativas.

3. DIRETRIZES

3.1. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Os princípios da segurança da informação abrangem, basicamente, os seguintes aspectos:

- **Integridade:** Garantia de que a informação seja mantida em seu estado original, precisa e completa, visando protegê-la, no processo, transporte e armazenamento, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Toda informação deve ser protegida conforme as regras definidas nesta Política. A adoção de procedimentos que garantam a segurança da informação deve ser prioridade constante nas áreas da Golden Cloud Technology, de forma que possam reduzir falhas e danos que venham a comprometer a imagem da empresa ou trazer prejuízos a outrem.

Informações produzidas ou recebidas pelos funcionários, estagiários e prestadores de serviço como resultado de sua atividade profissional ou em razão dela pertence à Golden Cloud Technology.

As exceções devem ser explícitas e formalizadas em um contrato entre as partes. Isso também se aplica aos equipamentos de informática, à comunicação, aos sistemas, a informações e a quaisquer recursos utilizados pelos funcionários para a realização das atividades profissionais. O uso dos recursos e equipamentos pessoais é permitido desde que esteja devidamente autorizado e não prejudique o desempenho dos sistemas e serviços da Golden Cloud Technology.

A Golden Cloud Technology, por meio da Segurança da Informação e outras áreas ligadas ao tema, poderá registrar e monitorar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas. Os critérios e requisitos estabelecidos nesta PSI deverão ser aplicados em todas as áreas da Golden Cloud Technology.

3.2. PROTEÇÃO DA INFORMAÇÃO

Define-se como necessária a proteção da informação da empresa, especialmente de sua propriedade, como fator primordial nas atividades profissionais de cada funcionário, estagiário e prestador de serviço da Golden Cloud Technology, sendo que:

- Devem assumir uma postura proativa no que diz respeito à proteção das informações da Golden Cloud Technology e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações e acesso indevido aos sistemas de informação sob responsabilidade da empresa;
- As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções e autorizações;
- Assuntos sigilosos classificados como confidenciais não devem ser expostos publicamente;
- Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;
- Somente softwares homologados podem ser utilizados no ambiente computacional da Golden Cloud Technology, em atendimento aos procedimentos de controle e aos critérios para a instalação de *softwares*;

- Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos. O descarte deve ser feito na forma da legislação ou diretriz pertinente;
- Todo usuário, para poder acessar dados das redes de computadores utilizadas pela Golden Cloud Technology, incluindo aquele que trabalhe de maneira remota, deverá possuir um login ou usuário de acesso atrelado à uma senha previamente cadastrada, pessoal e intransferível, ficando vedada a utilização de login ou usuário de acesso genérico ou comunitário, exceto previamente autorizado;
- Todo usuário deve ter acesso apenas às redes e aos serviços que tenham sido especificamente autorizados a usar, de modo a desempenhar, de maneira eficaz, as suas atividades;
- Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às permissões de acesso aplicáveis aos referidos dados;
- Os dados considerados como imprescindíveis aos objetivos da Golden Cloud Technology devem ser protegidos por meio de rotinas sistemáticas e documentadas de cópia de segurança, devendo ser submetidos aos testes periódicos de recuperação;
- O acesso físico às dependências da Golden Cloud Technology deve ser controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade e disponibilidade, garantindo a rastreabilidade e a efetividade do acesso autorizado;
- O acesso lógico aos sistemas computacionais disponibilizados pela Golden Cloud Technology deve ser controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade e disponibilidade da informação, garantindo a rastreabilidade e a efetividade do acesso autorizado;
- São de propriedade da Golden Cloud Technology todas as criações, códigos ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo com a empresa, nos limites legais (Leis nº 9.279/96, 9.609/98 e demais aplicáveis);

- Documentos imprescindíveis para as atividades da empresa deverão ser salvos em rede ou nuvem. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha, sendo, portanto, de responsabilidade do próprio funcionário;
- Arquivos pessoais e/ou não pertinentes às atividades diretas da Golden Cloud Technology não deverão ser copiados ou movidos para os drives de rede ou nuvem, pois podem sobrecarregar o armazenamento nos servidores. Caso identificados, os arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia ao funcionário;
- Os projetos gerenciados e realizados pela Golden Cloud Technology deverão adotar critérios de segurança da informação para o cumprimento desta política.

3.2.1. Prevenção contra Vazamento de Dados

Como parte do compromisso da Golden Cloud Technology com a proteção das informações e em conformidade com a ISO/IEC 27001, foi implementada uma solução robusta de Prevenção contra Vazamento de Dados (DLP) e Data Exfiltration. Através da ativação das funcionalidades de DLP no firewall FortiGate e DLP no Google Workspace para e-mail, é possível monitorar, filtrar e bloquear arquivos e dados sensíveis que circulam pelos sistemas da empresa, garantindo maior controle sobre o fluxo de informações.

3.2.1.1. DLP

A solução de DLP instalada permite:

- Monitoramento em tempo real de dados sensíveis, como informações pessoais, documentos confidenciais e dados financeiros, evitando sua exposição indevida;
- Aplicação de políticas de bloqueio automático para impedir o envio de dados não autorizados para fora da rede corporativa;
- Gerar relatórios sob demanda de forma customizada para necessidades como auditoria, possíveis vazamentos de dados e solicitações de áreas específicas,

garantindo a conformidade com as normas de segurança da informação e privacidade.

3.2.1.2. Data Exfiltration

A solução de Data Exfiltration permite:

- Identificação de padrões comportamentais que indicam possíveis tentativas de exfiltração de dados, como transferências não autorizadas para dispositivos externos, serviços de nuvem ou endereços IP desconhecidos.
- Análise em tempo real de atividades em *endpoints* para garantir que comportamentos anômalos sejam detectados antes de causar danos.
- Bloqueio automático de atividades não autorizadas, como uso de mídias removíveis e uploads para serviços não corporativos.
- Geração de logs detalhados para auditorias e conformidade com normas de segurança e regulamentações, como a LGPD.

Essa medida é fundamental para assegurar a integridade, confidencialidade e disponibilidade das informações da empresa, prevenindo incidentes de vazamento de dados e atendendo às exigências da Lei Geral de Proteção de Dados Pessoais (LGPD) e outras regulamentações aplicáveis.

3.2.2. Logs

A Golden Cloud Technology adota uma solução de coleta, gerenciamento, retenção e análise de logs, com o objetivo de garantir a segurança da informação e conformidade com padrões e regulamentações. Esta seção detalha como são tratados os logs dentro da empresa, destacando os tipos coletados, período de retenção, práticas de backup e geração de alarmes por meio do SIEM (*Security Information and Event Management*).

3.2.2.1. Tratamento de Logs

Os logs são coletados, processados e armazenados de maneira centralizada, seguindo as melhores práticas de segurança e integridade. O tratamento dos logs inclui:

- **Coleta**: Uso de agentes do SIEM instalados em dispositivos que possuem sistema operacional ou através do envio da função de Syslog em equipamentos físicos, garantindo a captura de eventos em tempo real.
- **Armazenamento seguro**: Os logs são armazenados em um servidor da ferramenta de SIEM com controle de acesso e backup ativo.
- **Análise**: Os dados são processados através da ferramenta de SIEM para identificar eventos suspeitos e correlacionar informações.

3.2.2.2. Tipos de logs coletados

A coleta de logs inclui, mas não se limita a:

- **Logs de segurança**: Registros de *firewall*, sistemas de prevenção de intrusão (IPS), autenticações e tentativas de acesso.
- **Logs de rede**: Tráfego de rede, VPN, DNS e *proxy*.
- **Logs de sistema**: Atividades de servidores, endpoints e dispositivos de rede.
- **Logs de aplicativos**: Eventos de aplicativos internos, bancos de dados e sistemas web.
- **Logs de auditoria**: Alterações em permissões, configurações e acessos administrativos.

3.2.2.3. Período de retenção

- **Retenção ativa**: Logs críticos são armazenados por 3 meses em ambientes de acesso rápido.
- **Arquivo histórico**: Os logs com a retenção maior que 3 meses são arquivados através da ferramenta de *backup* e pode ser retido por um período de até 5 anos, ou conforme regulamentações aplicáveis.

3.2.2.4. Políticas de backup

Os logs coletados são submetidos a uma política de *backup* de toda a estrutura da ferramenta de SIEM, que garante:

- **Backup diário incremental**: Armazenamento de alterações diárias para minimizar perda de dados.
- **Armazenamento redundante**: Backups mantidos em locais geograficamente distintos para prevenção de falhas.
- **Validação periódica**: Testes regulares de restauração para garantir a integridade e disponibilidade.

3.2.2.5. Equipamentos monitorados

A coleta de logs abrange uma ampla gama de dispositivos e sistemas, incluindo:

- *Firewalls*, *switches*, roteadores e balanceadores de carga.
- Servidores físicos e virtuais (Windows, Linux, etc.).
- Sistemas de armazenamento e *backup*.
- Ferramentas de segurança como *Endpoint Protection*.

3.2.2.6. Geração de alarmes no SIEM

Para identificação proativa de incidentes de segurança, os logs são analisados em tempo real por um sistema SIEM que:

- **Define regras de correlação**: Identifica padrões anômalos, como múltiplas tentativas de login ou acessos fora do horário normal.
- **Classifica eventos**: Organiza alertas por criticidade (alta, média, baixa).
- **Aciona alarmes**: Notifica automaticamente a equipe de SOC com a abertura de chamados de incidentes de segurança, *dashboards* com alertas em tempo real e integrações com ferramentas de resposta a incidentes.
- **Realiza ações automáticas**: Executa respostas ativas ou bloqueios preventivos em dispositivos afetados, conforme a gravidade do evento através das ferramentas de resposta a incidentes.

3.3. PRIVACIDADE DA INFORMAÇÃO

Define-se como necessária a privacidade das informações que são manipuladas ou armazenadas nos meios às quais a Golden Cloud Technology detém total controle

administrativo, físico, lógico e legal. As diretivas abaixo refletem os valores institucionais da Golden Cloud Technology e reafirmam o seu compromisso com a melhoria contínua desse processo:

- As informações são geradas, manipuladas, recebidas, tratadas e armazenadas de forma segura e íntegra, com métodos apropriados de segurança, podendo utilizar criptografia ou certificação digital, quando aplicável;
- As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;
- As informações podem ser disponibilizadas a quem tem direito de acesso, sendo exigido o cumprimento de nossa política e diretivas de segurança e privacidade de dados;
- As informações somente são fornecidas a terceiros, mediante autorização prévia da Golden Cloud Technology, do cliente ou para o atendimento de exigência legal ou regulamentar;
- As informações e dados constantes em cadastros da empresa, bem como outras solicitações que venham garantir direitos legais ou contratuais, só são fornecidos aos próprios interessados, mediante solicitação formal, seguindo os requisitos legais vigentes.

3.4. ESTRUTURA E CLASSIFICAÇÃO DA INFORMAÇÃO

A estrutura normativa e classificação das informações da Golden Cloud Technology define critérios de classificação de sensibilidade, administração e uso das informações do âmbito corporativo sobre roubo, perda, divulgação não-autorizada e uso indevido das informações que tragam prejuízos ao negócio ou risco de imagem institucional da Golden Cloud Technology, descrevendo como os sistemas e *softwares* que geram, armazenam e manipulam as informações, devem ser protegidos e utilizados.

3.5. ACESSOS

Define-se como necessário o controle de acesso da Golden Cloud Technology, de acordo com as seguintes diretrizes abaixo:

- O controle de acesso deverá considerar e respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação da Golden Cloud Technology;
- A criação e administração de contas será realizada de acordo com procedimento específico para todo e qualquer usuário. Para o usuário que não exerce funções de administração de rede, sistema ou qualquer atividade de gerenciamento, suporte e operação, será privilegiada a criação de uma única conta institucional de acesso, pessoal e intransferível. Contas com perfil de administrador somente serão criadas para usuários responsáveis pela execução de tarefas específicas na administração de ativos de informação;
- As práticas de segurança deverão contemplar procedimentos de acesso físico a áreas e instalações, gestão de acessos e delimitação de perímetros de segurança dos *data centers*;
- O uso do correio eletrônico da Golden Cloud Technology é para fins exclusivamente corporativos e relacionados às atividades da empresa.

3.6. REVISÕES DE ACESSOS

A área responsável pela gestão de acessos da Golden Cloud Technology deverá garantir que os processos críticos de concessão, transferência e revogação de acessos estejam sendo executados de acordo com o procedimento formal estabelecido no Sistema de Gestão Integrado. Os processos de revisão de acesso, físico, lógicos e críticos devem assegurar:

- A integridade: Garantia de que a informação seja mantida em seu estado original, precisa e completa, visando protegê-la no processo, transporte e armazenamento, contra alterações indevidas, intencionais ou acidentais.
- A confidencialidade: Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- A disponibilidade: Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

- O proprietário da informação: Prática dos princípios de "guarda" da informação, exercida pelos "proprietários" reflete-se nas revisões que esses "proprietários" têm que executar sobre os perfis de autoridade de acesso dentro dos sistemas. Em outras palavras, a equipe de Governança questionará ao "proprietário" se um acesso deve ser mantido ou removido durante o período de revisão. Os gestores revisam, aprovam ou solicitam alterações nos perfis de acesso dos cargos sob suas áreas de gestão.

Abaixo seguem as revisões executadas pela equipe de Governança:

3.6.1. Revisão de acessos – Desligados

Periodicamente, a equipe de Governança realiza a análise dos logins (acessos físicos e lógicos) ativos *versus* funcionários demitidos e emite um relatório da revisão de acessos desligados. Caso seja encontrado qualquer desvio na execução das análises, deve mitigar o incidente junto às equipes responsáveis, abrir um chamado de ação corretiva e acompanhar a sua resolução na ferramenta de ITSM.

3.6.2. Revisão de acessos – Físicos

Periodicamente, a equipe de Governança confronta as informações para verificação de ocorrência de qualquer tipo de desvio de acesso físico (acesso indevido).

3.6.3. Revisão de contas sem atividade

Periodicamente, a equipe de Governança deverá fazer a análise dos usuários que não acessam a rede há mais de 120 (cento e vinte) dias e emitir relatório da revisão dos usuários sem atividade aos responsáveis para validar se o acesso deverá continuar ativo ou ser revogado.

3.6.4. Revisão terceiros

Periodicamente, a equipe de Governança deverá fazer a análise de todos os Prestadores de Serviços e Terceiros ativos (acessos físicos e lógicos) na Golden Cloud

Technology, verificar junto aos gestores dos Prestadores de Serviços e Terceiros e validar se o acesso deverá continuar ativo ou se deverá ser revogado.

3.6.5. Revisão de contas genéricas

Periodicamente, a equipe de Governança deverá fazer a análise de todas as contas genéricas, de serviço e administrativas de gestão de serviços para o ambiente interno (corporativo) e externo (clientes), verificar junto aos responsáveis/equipes responsáveis e validar se o acesso deverá continuar ativo ou se deverá ser desativado.

3.7. BACKUP

Define-se como necessário, as seguintes diretrizes da Golden Cloud Technology:

- O serviço de *backup* deve ser aplicado por ferramentas próprias considerando, inclusive, a execução agendada fora do horário de expediente normal da empresa, se possível, nas chamadas "janelas de *backup*" – períodos em que não há nenhum ou há pouco acesso de funcionários ou processos automatizados aos sistemas de informação;
- A solução de *backup* deverá ser mantida atualizada, considerando suas diversas características (atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros);
- A administração das mídias de *backup*, quando aplicável, deverá ser contemplada nas normas complementares sobre o serviço, objetivando manter sua segurança e integridade;
- As mídias de *backups* históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de cofres e salas-cofres;
- Os *backups* críticos, para o bom funcionamento dos serviços da Golden Cloud Technology, exigem uma regra de retenção especial, a ser prevista nos procedimentos específicos e de acordo com as normas estabelecidas, seguindo ainda as determinações fiscais e legais existentes no País;

- A execução de rotinas de *backup* e *restore* deverá ser controlada nos termos do documento "GCLOUD_SGI_PG_025_Gestão de Backup e Restore".

3.8. DATA CENTER

Definem-se como necessárias as seguintes diretrizes da Golden Cloud Technology:

- A administração de dados e de serviços de *data center* é uma tarefa tecnicamente complexa e sua realização deve balizar-se nas melhores práticas de mercado e na alocação de profissionais com perfil técnico adequado;
- O acesso físico ao data center por meio de recursos mecânicos-manuais apenas poderá ocorrer em situações de emergência, quando a segurança física do data center estiver comprometida, como incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando;
- O acesso ao *data center* por visitantes ou terceiros somente poderá ser realizado com autorização de um funcionário da Golden Cloud Technology com a devida permissão de acesso ao *datacenter*, que deverá preencher a solicitação de acesso prevista, conforme estabelecida na norma própria;
- Deverá ser executada, em frequência predeterminada, auditoria dos acessos ao *data center* – por meio de relatório do sistema de registro próprio;
- A lista de funções com direito de acesso ao *data center* deverá ser constantemente atualizada, de acordo com os termos de norma própria, salva em locais seguros e apropriados;
- No caso de desligamento de usuários que possuam acesso ao *data center*, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação e da lista de usuários autorizados.

3.9. MONITORAMENTO E AUDITORIA DO AMBIENTE

Define-se como necessário a existência de mecanismos de monitoramento e auditoria da Golden Cloud Technology para:

- Permitir o monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou *wireless* e outros componentes da

rede, de modo que a informação gerada por esses sistemas possa ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

- Tornar disponível as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Departamento Jurídico;
- Realizar, a qualquer tempo, inspeção física e/ou lógica nas informações de propriedade da Golden Cloud Technology;
- Realizar, a qualquer tempo, inspeção nos equipamentos de propriedade da Golden Cloud Technology, a fim de identificar se os locais de instalação estão adequados para reduzir os riscos de ameaça, os perigos do meio ambiente, as oportunidades de acesso não autorizado, as possibilidades de falta de energia elétrica e de intercepção, interferência ou danos.
- Permitir mecanismos e práticas de proteção preventivos, detectáveis ou corretivos para garantir segurança das informações e dos perímetros de acesso físico;
- Desinstalar, a qualquer tempo, qualquer *software* ou sistema que represente risco ou esteja em não conformidade com as políticas, normas e procedimentos vigentes.

3.10. EXCLUSÃO DE DADOS

A exclusão de dados é uma prática essencial para garantir a conformidade com políticas de retenção, otimização de recursos e proteção da privacidade e segurança das informações. A Golden Cloud Technology adota controles rigorosos para a exclusão de dados em diferentes áreas de sua infraestrutura, conforme detalhado a seguir.

3.10.1. Exclusão de Dados em Virtualizadores

No ambiente virtualizado, a exclusão de dados é realizada seguindo um processo seguro e controlado para prevenir acessos não autorizados e assegurar a integridade do ambiente.

- **Procedimentos de Exclusão:**

- Antes da exclusão, *snapshots* e discos virtuais associados a VMs obsoletas são identificados e analisados.
- A remoção é realizada utilizando ferramentas nativas da solução de virtualização utilizada, que garantem a exclusão permanente dos dados do armazenamento.
- O armazenamento liberado passa por processos de zero-fill ou sobrescrita, dependendo da criticidade dos dados, impedindo a recuperação de informações sensíveis.

- **Auditoria**:
  - Logs detalhados das exclusões são gerados e armazenados em ferramenta de SIEM para revisão em auditorias internas e externas.

3.10.2. Exclusão de Dados de Backup

Os dados de *backup* seguem uma política de retenção rigorosa, respeitando prazos definidos conforme as necessidades contratuais e regulamentares.

- **Procedimentos de Exclusão:**
  - Dados cuja retenção expira são identificados automaticamente pela ferramenta de gerenciamento de *backups*, seguindo as políticas configuradas.
  - A exclusão ocorre de forma automatizada, com validação pelo sistema de que o processo foi concluído.
  - Para *backups* confidenciais ou de alta criticidade, uma validação adicional por um administrador é realizada antes da exclusão.
- **Segurança**:
  - A ferramenta onde os *backups* são gerenciados utiliza algoritmos de exclusão que garantem a destruição lógica e física dos dados no armazenamento subjacente, eliminando a possibilidade de recuperação.

3.10.3. Exclusão de Dados de Migrações de Ambientes de Clientes

Para dados temporários resultantes de migrações de clientes, é utilizada uma abordagem automatizada para evitar o armazenamento desnecessário no ambiente.

- **Procedimentos de Exclusão:**
  - Os dados de migração são armazenados em diretórios específicos durante o processo.
  - Um script automatizado é executado regularmente, identificando e excluindo arquivos com mais de 90 dias de existência.
  - Este processo reduz a ocupação de espaço e minimiza os riscos associados à retenção de informações sensíveis.
- **Configuração do Script:**
  - O script verifica diretórios predefinidos, analisa timestamp de arquivos (data de criação ou modificação) e realiza a exclusão de maneira segura.
  - Logs do processo, com registro do que foi excluído e quando, são gerados e armazenados para fins de auditoria e rastreamento.
- **Segurança**:
  - Os arquivos são excluídos permanentemente, com validação de que nenhum dado residual permanece no ambiente.

3.11. USO E ACESSO À INTERNET

Definem-se como necessárias as seguintes diretrizes da Golden Cloud Technology:

- Qualquer informação que seja acessada, transmitida, recebida ou produzida na internet está sujeita à monitoria e auditoria. Portanto, a Golden Cloud Technology, em total conformidade legal, reserva-se o direito de monitorar e registrar os acessos à internet de todos os funcionários e prestadores de serviço;
- Todos os usuários, durante o uso e acesso à internet, devem respeitar os controles de detecção, prevenção e recuperação para proteção contra *malware;*
- Os equipamentos, tecnologias e serviços fornecidos para o acesso à internet são de propriedade da Golden Cloud Technology, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando a assegurar o cumprimento de sua Política de Segurança da Informação.

3.11.1. Filtragem web

A Golden Cloud Technology utiliza a filtragem web como mecanismo fundamental no gerenciamento de acesso a sites externos, com o objetivo de reduzir a exposição a conteúdos maliciosos e garantir um ambiente digital seguro e produtivo. Esse controle é aplicado tanto para dispositivos corporativos quanto para computadores pessoais utilizados no âmbito da empresa, *Bring Your Own Device* (BYOD), protegendo os colaboradores e os ativos digitais da organização.

3.11.1.1. Gerenciamento de acesso

A filtragem é realizada por meio de soluções especializadas que classificam e restringem o acesso a sites com base em categorias, reputação ou políticas personalizadas definidas pela empresa. Os bloqueios também são definidos para grupos distintos de acordo com o perfil de colaboradores ou setores específicos. Os principais bloqueios são:

- Sites de entretenimento de jogos;
- Sites de namoros;
- Sites relacionados a drogas;
- Sites relacionados a nudez e outros materiais adultos;
- Sites de pornografia;
- Sites de vendas de armas.

3.11.1.2. Cobertura de dispositivos

- Dispositivos Corporativos: Todo tráfego é monitorado e controlado diretamente pela infraestrutura da empresa, incluindo computadores, notebooks e dispositivos móveis corporativos.
- Dispositivos Pessoais (BYOD): Para computadores pessoais que acessam a rede ou sistemas da empresa, o controle é feito por agentes instalados no dispositivo, estendido por meio de integrações como redes de *firewalls* e VPNs, ou por perímetro se necessário.

3.11.1.3. Mecanismos de monitoramento

- Ferramentas de segurança inspecionam o tráfego em tempo real, detectando e bloqueando atividades que representem riscos à segurança da informação.

- Logs são mantidos para auditoria e análise de eventos suspeitos, possibilitando resposta rápida a incidentes.

3.11.1.4. Acessos e exceções

O acesso é definido pelo time de Segurança da Informação, com regras claras sobre os tipos de sites permitidos e bloqueados. Exceções podem ser avaliadas caso a caso, mediante justificativa formal, garantindo flexibilidade para atividades corporativas legítimas.

3.11.1.5. Responsabilidade dos usuários

Todos os colaboradores, independentemente do dispositivo utilizado, devem:

- Respeitar as restrições impostas pela política de filtragem web.
- Evitar tentativas de burlar os controles estabelecidos.
- Reportar imediatamente qualquer incidente ou comportamento anômalo relacionado ao acesso web.

3.11.1.6. Ferramentas utilizadas

A infraestrutura utiliza soluções de filtragem web integradas a sistemas de proteção através de *firewall* e agentes de segurança de *endpoint protection*, assegurando cobertura ampla e eficiente contra ameaças cibernéticas.

3.12. GESTÃO DE RISCOS

As diretrizes gerais de gestão de riscos do Sistema de Gestão Integrado (SGI) da Golden Cloud Technology deverão considerar, prioritariamente, os objetivos estratégicos e financeiros, os processos críticos, os requisitos legais e a estrutura da empresa.

A gestão de riscos da Golden Cloud Technology está formalizada no documento GCLOUD_SGI_PG_032_Gestão de Riscos.

3.13. TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Definem-se como necessárias as seguintes diretrizes da Golden Cloud Technology:

- Todos os incidentes de segurança da informação notificados ou detectados deverão ser registrados e relatados por meio dos canais de gestão, com a finalidade de

assegurar o histórico das atividades desenvolvidas e de reduzir a probabilidade ou o impacto de incidentes futuros;

- O tratamento de incidentes de segurança da informação deverá ser realizado de forma a viabilizar e assegurar disponibilidade, integridade e confidencialidade da informação, observando a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo;
- Durante o gerenciamento de incidentes de segurança da informação, havendo indícios de ilícitos criminais, a equipe de Governança, o departamento de Gestão de Pessoas, o departamento Jurídico ou membros das equipes técnicas ligados às atividade de segurança da Informação têm como dever, sem prejuízo de suas demais atribuições, acionar as autoridades competentes para a adoção dos procedimentos legais julgados necessários, observar os procedimentos para preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia, e priorizar a continuidade dos serviços da Golden Cloud Technology.

3.14. AUDITORIAS

Toda informação confidencial sob responsabilidade da Golden Cloud Technology é passível de auditoria, conforme descrito nos documentos abaixo, em data e horários determinados pela equipe de Governança, ou outras áreas ligadas ao tema, podendo também, ocorrer sem aviso prévio.

- Programa de Auditoria;
- Plano de Auditoria Interna;
- GCLOUD_SGI_PG_005_Auditoria Interna do SGI;
- GCLOUD_SGI_PG_008_Gestão de Não Conformidades e Melhorias.

A realização de auditoria para o SGI deverá ser, obrigatoriamente, coordenada pela equipe de Governança e, durante a sua execução, deverá ser resguardado o sigilo de dados pessoais e pessoais sensíveis, desde que não estejam dispostos em ambiente físico ou lógico de propriedade da Golden Cloud Technology. Durante a auditoria, o acesso às informações

de propriedade ou sob responsabilidade da organização que não tenha sido previamente protegida por um termo confidencialidade deve ser impedido.

3.15. SEGURANÇA DA INFORMAÇÃO NO FORNECIMENTO E USO DE SERVIÇO EM NUVEM

Quando a Golden Cloud Technology provê serviços em nuvem, as seguintes questões devem ser consideradas, a fim de implementar a segurança da informação para o seu fornecimento e uso desses serviços:

- Requisitos básicos de segurança da informação aplicáveis à concepção e implementação do serviço em nuvem;
- Riscos de acesso por pessoas internas autorizadas;
- Isolamento dos multi locatários e do cliente do serviço em nuvem (incluindo virtualização);
- Acesso aos ativos de clientes de serviços em nuvem pelos funcionários da Golden Cloud Technology;
- Procedimentos de controle de acesso, como autenticação forte para acesso administrativo aos serviços em nuvem;
- Comunicações para clientes do serviço em nuvem durante a gestão da mudança;
- Segurança da virtualização;
- Acesso e proteção dos dados de clientes do serviço em nuvem;
- Gestão do ciclo de vida das contas de clientes do serviço em nuvem;
- Comunicação de violações e diretrizes para compartilhamento de informação visando auxiliar investigações e análise forense.

3.16. REGULAMENTAÇÃO E LEGISLAÇÃO APLICÁVEIS

A Golden Cloud Technology monitora as leis, obrigações e deveres estatutários, regulatórios, contratuais e profissionais que possam impactar o negócio e as partes interessadas. O monitoramento é realizado pelo time jurídico em uma base anual, através de pesquisas e recebimento de notificações de órgãos responsáveis. Os dispositivos regulatórios aplicáveis, incluindo as atualizações legislativas de cada um, à Golden Cloud Technology atualmente são:

- Código Penal - Decreto-Lei nº 2.848/1940;
- Código Civil - Lei Federal nº 10.406/2002;
- Código Tributário Nacional - Lei nº 5.172/1966;
- Consolidação das Leis do Trabalho - Decreto-Lei nº 5.452/1943;
- Constituição da República Federativa do Brasil de 1988;
- Estatuto da Pessoa com Deficiência - Lei nº 13.146/2015;
- Lei Anticorrupção - Lei nº 12.846/2013;
- Lei Antitruste - Lei nº 12.529/2011;
- Lei de Direitos Autorais - Lei nº 9610/1998;
- Lei das Estatais - Lei nº 13.303/2016;
- Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018;
- Lei da Igualdade Salarial - Lei nº 14.611/2023;
- Lei de Licitações - Lei nº 14.133/2021;
- Lei de Marcas e Patentes - Lei nº 9.279/1996;
- Lei dos Planos de Benefícios da Previdência Social e dá outras providências - Lei nº 8.213/1991;
- Lei de Propriedade Intelectual de Programa de Computador - Lei nº 9.609/1998;
- Marco Civil da Internet - Lei nº 12.965/2014;
- Decreto nº 8.771/2016, que regulamenta o Marco Civil da Internet quanto à segurança e guarda de registros.
- Norma Regulamentadora Nº 4 (NR-4). Serviços Especializados em Segurança e em Medicina do Trabalho;
- Norma Regulamentadora Nº 5 (NR-5). Comissão Interna de Prevenção de Acidentes;
- Norma Regulamentadora Nº 7 (NR-7). Programa de Controle Médico e Saúde Ocupacional - PCMSO;
- Norma Regulamentadora Nº 9 (NR-9). Avaliação e Controle das Exposições Ocupacionais a Agentes Físicos, Químicos e Biológicos;

- ABNT NBR ISO/IEC 27001 – 2022 – Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos
- ABNT NBR ISO/IEC 31000 – 2018 – Gestão de Riscos – Princípios e Diretrizes.
- ABNT NBR ISO/IEC 27017 – 2016 – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem
- ABNT NBR ISO/IEC 27018 – 2018 – Tecnologia da informação — Técnicas de segurança — Código de prática para proteção de informações de identificação pessoal (PII) em nuvens públicas que atuam como processadores de PII.
- ABNT NBR ISO/IEC 27701 – 2019 – Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes
- ABNT NBR ISO/IEC 20000-1:2018 – Requisitos para sistemas de gestão de serviços de TI

O Sistema de Gestão Integrado estabelece responsabilidade, regras e realiza ações de melhorias para evitar violações a aspectos legais e regulamentares de requisitos de segurança da informação, sendo elas:

- Decisões que incluem obrigações legais;
- Projeções de custo-benefício para o sistema de gestão e serviços;
- Análise de risco e benefícios intangíveis para o sistema de gestão e serviços, bem como suas obrigações éticas com o conteúdo dos dados.

4. PAPÉIS E RESPONSABILIDADES

A seguir estão relacionadas às responsabilidades e obrigações que deverão ser cumpridas por cada área da Golden Cloud Technology.

4.1. FUNCIONÁRIOS, ESTAGIÁRIOS E PRESTADORES DE SERVIÇOS

Cabe aos funcionários, estagiários e prestadores de serviço da Golden Cloud Technology cumprir com as seguintes obrigações:

- Zelar continuamente pela proteção das informações da Golden Cloud Technology, especialmente as confidenciais, sendo contra acesso, modificação, destruição ou divulgação não autorizada;
- Buscar orientação do superior imediato e/ou das áreas de negócio, especialmente equipe de Governança, Gestão de Pessoas, Jurídico, Segurança da Informação ou TI Corporativa, em caso de dúvidas relacionadas à Segurança da Informação;
- Assinar o termo de sigilo e confidencialidade, formalizando a ciência e o aceite das Políticas e Normas de Segurança da Informação, bem como assumindo a responsabilidade por seu cumprimento;
- Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados primariamente para fins profissionais da Golden Cloud Technology;
- Participar dos treinamentos, palestras e apresentações, presenciais ou virtuais, de Segurança da Informação que são disponibilizados;
- Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas para o negócio;
- Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
- Atender às leis que regulamentam as atividades da empresa e seu mercado de atuação;
- Selecionar de maneira coerente os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;
- Comunicar imediatamente à equipe de Governança, departamento de Gestão de Pessoas, departamento Jurídico ou TI Corporativa qualquer descumprimento da Política de Segurança da Informação e/ou das normas relacionadas.

4.2. FORNECEDORES

Cabe aos fornecedores da Golden Cloud Technology cumprir com as seguintes obrigações:

- Assinar cláusula de confidencialidade em contrato, e em caso de fornecedores estratégicos, formalizar a ciência e estar de acordo com as Política de Segurança da Informação, Código de Ética e Conduta Profissional, Política Anticorrupção e Antissuborno, Política Geral de Proteção de Dados Pessoais e Aviso de Privacidade da Golden Cloud Technology.

4.3. COMITÊ DO SISTEMA DE GESTÃO INTEGRADO

O Comitê do Sistema de Gestão Integrado (CSGI) é um grupo multidisciplinar que reúne, quando necessário, representantes de distintas áreas da Golden Cloud Technology, composto por indicados e aprovados pelas suas respectivas lideranças. Esse comitê deve deliberar sobre assuntos referentes à Segurança da Informação, qualidade, satisfação do cliente e continuidade de negócios que gerem impactos ou influências no negócio. Assim, compete ao CSGI:

- Propor ajustes, aprimoramentos e modificações na estrutura normativa, submetendo à avaliação da Alta Direção;
- Promover a Segurança da Informação na organização, aprovando as políticas do Sistema de Gestão Integrado da Golden Cloud Technology;
- Requisitar informações das demais áreas da organização, por meio das diretorias e gerências, com o intuito de verificar o cumprimento das políticas e normas do Sistema de Gestão Integrado da Golden Cloud Technology;
- Receber, analisar e notificar as gerências e diretoria, quanto a casos de violação da política e das normas do Sistema de Gestão Integrado da Golden Cloud Technology;
- Estabelecer mecanismos de registro e controle de eventos e incidentes de segurança da informação, bem como, de não conformidades das políticas, normas ou dos procedimentos do Sistema de Gestão Integrado da Golden Cloud Technology;
- Acompanhar o andamento dos projetos e iniciativas relacionados ao Sistema de Gestão Integrado;
- Realizar, sistematicamente, a gestão de riscos relacionados ao Sistema de Gestão Integrado.

4.4. DIRETORIA (ALTA DIREÇÃO)

Cabe à Diretoria ou Alta Direção:

- Prover os recursos necessários para garantir a eficácia do CSGI;
- Assessorar o CSGI quanto a qualquer decisão relacionada ao Sistema de Gestão Integrado (SGI);
- Apoiar as políticas, as diretrizes e as normas do Sistema de Gestão Integrado da Golden Cloud Technology;
- Receber relatórios de violações da política, diretrizes e das normas do Sistema de Gestão Integrado da Golden Cloud Technology, quando aplicável;
- Receber relatórios de não conformidades do CSGI;
- Realizar a análise crítica do SGI.

4.5. LÍDER DA ÁREA OU DEPARTAMENTO

Cabe ao líder da área ou departamento cumprir as seguintes obrigações:

- Cumprir e fazer cumprir a política, as normas e procedimentos do Sistema de Gestão Integrado da Golden Cloud Technology;
- Assegurar que a sua equipe possua acesso e entendimento de políticas, normas, planos, processos e procedimentos do Sistema de Gestão Integrado e da Golden Cloud Technology;
- Sugerir a Segurança da Informação ou ao CSGI, de maneira proativa, procedimentos de segurança da informação relacionados às suas áreas;
- Redigir e detalhar, tecnicamente e operacionalmente, as normas e procedimentos do Sistema de Gestão Integrado da Golden Cloud Technology relacionados à sua área, quando solicitado;
- Comunicar imediatamente à equipe de Governança eventuais casos de violação da política, de normas ou de procedimentos do Sistema de Gestão Integrado da Golden Cloud Technology;
- Incentivar que políticas, normas, planos, processos e procedimentos do Sistema de Gestão Integrado da Golden Cloud Technology sejam cumpridos de acordo com os preceitos definidos para a sua área de atuação;

- Criar, atualizar e gerenciar os procedimentos que estão sob sua responsabilidade;
- Armazenar evidências dos processos, assim como fornecê-las quando solicitado pela equipe de Governança;
- Incluir na análise e elaboração de projetos internos ou com clientes, fornecedores, prestadores de serviços e parceiros de negócio, sempre que necessário e quando aplicável, avaliações específicas relacionadas à segurança da informação e continuidade de negócio, com o objetivo de proteger os interesses e ativos críticos da Golden Cloud Technology.

4.6. PROPRIETÁRIO DA INFORMAÇÃO

O proprietário da informação é o líder do departamento ou área da Golden Cloud Technology, considerando diretor, gerente, coordenador, líder, supervisor ou chefe de equipe, responsável pela aprovação, revisão, orientação na classificação da informação e cancelamento de autorizações de acesso a determinado conjunto de informações sob a sua guarda.

4.7. DEPARTAMENTO JURÍDICO

Cabe ao departamento Jurídico:

- Manter as áreas e departamento da Golden Cloud Technology informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e ações envolvendo o Sistema de Gestão Integrado;
- Incluir na análise e elaboração de contratos de clientes, fornecedores, prestadores de serviços e parceiros de negócio, sempre que necessário e quando aplicável, cláusulas específicas relacionadas à Segurança da Informação, com o objetivo de proteger os interesses da organização;
- Avaliar, quando solicitado pelas áreas ligadas ao tema, as políticas, diretrizes, normas e procedimentos do Sistema de Gestão Integrado da Golden Cloud Technology;
- Auxiliar o CSGI e a equipe de Governança nas demais questões legais.

4.8. GESTÃO DE PESSOAS

Cabe à área de Gestão de Pessoas:

- Assegurar-se de que os funcionários comprovem, por escrito, estar cientes da estrutura normativa do SGI e dos documentos que a compõem, como por exemplo, através da assinatura do Termo de Ciência e Compromisso;
- Criar mecanismos para informar, antecipadamente aos fatos, ao canal de atendimento técnico mais adequado, alterações no quadro funcional da Golden Cloud Technology;
- Promover as campanhas de treinamento, palestras e conscientização, presencial ou virtual, para todas as áreas e unidades da Golden Cloud Technology;
- Obter a assinatura do Termo de Sigilo e Confidencialidade dos funcionários, arquivando-os nos respectivos ambientes de registro.

4.9. EQUIPE DE GOVERNANÇA

Cabe à equipe de Governança:

- Aprovar a composição do CSGI da Golden Cloud Technology;
- Consolidar, manter e coordenar a elaboração, evolução, acompanhamento e avaliação do CSGI;
- Convocar, coordenar e prover apoio às reuniões do CSGI;
- Prover as informações de segurança quando solicitadas pelo CSGI;
- Facilitar a conscientização, a divulgação e o treinamento quanto às políticas, normas, planos, processos e procedimentos do Sistema de Gestão Integrado e da Golden Cloud Technology;
- Executar projetos e iniciativas visando a otimizar a Segurança da Informação para a Golden Cloud Technology;
- Conduzir a gestão, avaliação e tratamento de risco ligados ao Sistema de Gestão Integrado;
- Analisar, auditar e promover a Segurança da Informação, assim como, novos regulamentos, legislações e novas certificações na Golden Cloud Technology ligados ao Sistema de Gestão Integrado;

- Apoiar na criação e revisão dos procedimentos de Segurança da Informação dentro do escopo do CSGI e do Sistema de Gestão Integrado;
- Realizar rondas, vistorias, auditorias e análise crítica do escopo do Sistema de Gestão Integrado, emitindo relatório para o CSGI e a alta direção;
- Atuar como ponto de orientação para outras equipes e gerências em assuntos relacionados à Segurança da Informação.

5. PENALIDADES

São consideradas violações à política, às diretrizes, às normas e aos procedimentos do Sistema de Gestão Integrado as seguintes situações, não se tratando de rol taxativo:

- Quaisquer ações ou situações que possam expor a Golden Cloud Technology à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos críticos de informação;
- Utilização indevida de dados corporativos, divulgação não autorizada de informações, segredos comerciais ou outras informações confidenciais sem a permissão expressa do Líder/Proprietário da Informação;
- Uso de dados, imagens, informações, equipamentos, *software*, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos como o documento “GCLOUD_SGI_NO_001_Código de Ética e Conduta Profissional” e externos ou de exigências de organismos reguladores da área de atuação da Golden Cloud Technology;
- A não comunicação imediata às áreas de gestão sobre quaisquer descumprimentos da política, dos critérios, de normas ou de procedimentos de Segurança da Informação, que porventura um funcionário venha a tomar conhecimento ou chegue a presenciar.

O não cumprimento dos requisitos previstos nesta política, nas normas complementares e nos procedimentos de Segurança da Informação, acarretará violação às

regras internas da empresa e sujeitará o funcionário às medidas administrativas e legais cabíveis, podendo envolver advertência, suspensão, rescisão contratual ou outras medidas apropriadas conforme legislação vigente, como, por exemplo, a aplicação do artigo 482 da CLT.

6. CONTROLE DE REGISTROS

NOME DO REGISTRO	LOCAL DE ARMAZENAMENTO	TEMPO DE RETENÇÃO		RECUPERAÇÃO
		ATIVO	INATIVO	
GCLOUD_SGI_PO_001_Política de Segurança da Informação	Base de Conhecimento na Ferramenta de ITSM	Permanente	N/A	*Commvault Backup*

7. CONTROLE DE REVISÕES

HISTÓRICO DE REVISÕES		
DATA	**COMENTÁRIOS**	**REVISADO/ APROVADO POR:**
01/09/2020	Elaboração do documento	Ricardo Gomes / Jefferson Farias
15/07/2021	Revisão completa do documento	Rafael Moura / Jefferson Farias
24/08/2021	Revisão completa do documento	Rafael Moura / Jefferson Farias
27/10/2021	Inclusão de papéis e responsabilidades dos fornecedores	Rafael Moura / Ricardo Gomes
22/09/2022	Reestruturação de layout do documento	Viviane Sombra / Ricardo Gomes
11/11/2022	Ajuste de nomenclatura de documentos citados e inclusão de lei	Viviane Sombra / Ricardo Gomes
25/07/2023	Revisão de layout	Viviane Sombra / Ricardo Gomes
01/09/2023	Revisão completa do documento	Andressa Farias/ Jefferson Farias

23/08/2024	Revisão completa do documento	Cristian Nascimento / Jefferson Farias
17/10/2024	Revisão do documento e inclusão de informações no item 3	Edmar Ferraz / Jefferson Farias
03/12/2024	Complemento de informações no item 3.2.1	Edmar Ferraz / Jefferson Farias
05/09/2025	Revisão completa do documento e atualização do layout	Edmar Ferraz / Jefferson Farias