

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 27002:2013, 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 a assegurar a confidencialidade, disponibilidade e integridade do processamento, transferência, manuseio e armazenamento das informações críticas que estão no escopo do SGI.

Os objetivos definidos nesta Política são:

- Manter avaliações de riscos de Segurança da Informação dentro do escopo do SGI de acordo com o Procedimento de Gestão de Riscos da GOLDEN CLOUD TECHNOLOGY;
- Manter os níveis aceitáveis de risco residual para a organização;
- Garantir níveis aceitáveis de confidencialidade, integridade e disponibilidade das informações críticas;
- Atender aos requisitos regulamentares e legislativos;
- Realizar a conscientização da Segurança da Informação para todos os funcionários, estagiários e prestadores de serviço da GOLDEN CLOUD TECHNOLOGY;
- Relatar a avaliação de todas as violações da segurança da informação e vulnerabilidades para as partes interessadas;

- Apoiar a manutenção das normas do Sistema de Gestão Integrado: ISO 27001 – Gestão da Segurança da Informação, ISO 27017 – Segurança da Informação para Provedores e Clientes de Serviços em Nuvem e ISO 27018 – Proteção de Informações de Identificação Pessoal (PII) em Nuvens Públicas.

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 suas políticas, diretrizes, normas 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, visando a protegê-la, no processo, transporte e armazenamento, contra alterações indevidas, intencionais ou acidentais.

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

- **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.

Toda informação produzida ou recebida 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 pessoal dos recursos e equipamentos 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 da GOLDEN CLOUD TECHNOLOGY , sendo que:

- Os funcionários devem assumir uma postura proativa no que diz respeito à proteção das informações da GOLDEN CLOUD TECHNOLOGY e devem estar atentos a ameaças

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

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 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;
- Todos 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,

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

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.

3.3. 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;

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

- 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 de nossos cadastros, 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 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 cadastrados para 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 processo 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, 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.
- 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

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

Periodicamente, a equipe de Governança deverá fazer a análise dos logins ativos x funcionários demitidos (Gestão de Pessoas) e emitir um relatório da revisão de acessos desligados. Caso seja encontrado qualquer desvio na execução das análises, deverá mitigar o incidente junto às equipes responsáveis, abrir um ticket de ação corretiva e acompanhar a sua resolução no sistema de chamados.

3.6.2. Revisão de acessos – Físicos

Periodicamente, a equipe de Governança confrontará 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 , emitir relatório para os 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), emitir relatório para os 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:

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

- 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 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 “GCLLOUD_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* deverá ser feito por um sistema forte de autenticação. O acesso físico 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;

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

- O acesso ao *data center* por visitantes ou terceiros somente poderá ser realizado com autorização de um funcionário da GOLDEN CLOUD TECHNOLOGY, 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 e 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 interceptação, interferência ou danos.
- Permitir mecanismos e práticas de proteção preventivos, detectáveis ou corretivos para garantir segurança das informações e dos perímetros de acesso físico;

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

- 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. 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;
- Todos os usuários, durante o uso e acesso à internet, devem respeitar os controles de detecção, prevenção e recuperação para proteger 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. 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.

Toda a gestão de risco da GOLDEN CLOUD TECHNOLOGY está formalizada no documento GCLLOUD_SGI_PG_032_Gestão de Riscos.

3.12. 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

Cód.: GCLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

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 Governança, o Departamento de Gestão de Pessoas o Departamento Jurídico ou membros da Equipe Técnica ligadas 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 .

3.13. 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.

- Plano de Auditoria Interna;
- GCLOUD_SGI_PG_005_Auditoria Interna do SGI;
- GCLOUD_SGI_PG_008_Gestão de Não Conformidades e Oportunidades de Melhoria.

A realização de auditoria para o SGI deverá ser, obrigatoriamente, coordenada pela equipe de Governança e, durante a sua execução, deverão ser resguardados os direitos quanto à privacidade de informações pessoais, desde que essas não estejam dispostas em ambiente físico ou lógico de propriedade da GOLDEN CLOUD TECHNOLOGY e impedindo o acesso às informações de propriedade ou sob responsabilidade da organização.

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

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

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 dos clientes do serviço em nuvem;
- Comunicação de violações e diretrizes para compartilhamento de informação para auxiliar investigações e análise forense.

3.15. REGULAMENTAÇÃO E LEGISLAÇÃO APLICÁVEIS

Correlacionam-se com a Política, diretrizes e normas do Sistema de Gestão Integrado as leis abaixo relacionadas, mas não se limitando às mesmas:

- CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988;
- CÓDIGO TRIBUTÁRIO NACIONAL pelo art. 7º do Ato Complementar nº 36, de 13.3.1967;
- CONSOLIDAÇÃO DAS LEIS DO TRABALHO -DECRETO-LEI N.º 5.452, DE 1º DE MAIO DE 1943 alterada pela Lei Federal 13.467/2017;
- Lei Federal 10406, de 10 de janeiro de 2002 (Institui o Código Civil);
- Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código Penal);

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

- Lei Federal 9983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências);
- LEI Nº 9.472, DE 16 DE JULHO DE 1997;
- Lei de direito autoral Nº 9610/98;
- Lei de marcas e patentes Nº 9.279 de 14/05/1996;
- Lei das telecomunicações Nº 9.472 de 16/07/1997;
- Lei de propriedade intelectual de programa de computador Nº 9.609 de 19/02/1998;
- LEI Nº 12.737 - Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
- Lei Nº 12.965 de 23/04/2014 (Marco Civil da Internet).
- Lei 8666/95 - Lei de Licitação
- Lei 14.133/2021 - Nova Lei de Licitação
- Lei 12.846 - Lei anticorrupção
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais
- ABNT NBR ISO/IEC 27001 – 2013 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos, alterada pela NBR ISO/IEC 27002 DE 10/2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação.
- ABNT NBR ISO/IEC 27005 - 2008 - Tecnologia de Informação - Técnicas de segurança - Gestão de riscos de segurança da informação
- ABNT NBR ISO/IEC 31000 – 2009 – Gestão de Riscos – Princípios e Diretrizes.
- Lei Geral de Proteção de Dados – 13.709

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, contra acesso, modificação, destruição ou divulgação não autorizada;
- Buscar orientação do superior imediato e/ou das áreas, especialmente Equipe Governança, Gestão de Pessoas, Jurídico 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;

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

- 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

- Assinar o termo de sigilo e confidencialidade, formalizando a ciência e o aceite das Políticas e Normas de Segurança da Informação, bem como o Termo de Compromisso com as políticas de segurança 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 representantes de diversas 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 do Sistema de Gestão Integrado;

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

- 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 da política, das normas e dos 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;

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

- Incentivar que a Política, normas 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, as diretrizes, as normas e procedimentos do Sistema de Gestão Integrado da GOLDEN CLOUD TECHNOLOGY;

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

- 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, o 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-o nos respectivos prontuários.

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 à política, às normas e os 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;

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

- 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;
- Criar e revisar os 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 “GCLLOUD_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 cabíveis 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	
GCLLOUD_SGI_PO_001_Política de Segurança da Informação	Base de Conhecimento na Ferramenta de ITSM	Permanente	N/A	<i>Commvault Backup</i>
GCLLOUD_SGI_PG_032_Gestão de Riscos	Base de Conhecimento na Ferramenta de ITSM	Permanente	N/A	<i>Commvault Backup</i>
GCLLOUD_SGI_PG_025_Gestão de Backup e Restore	Base de Conhecimento na Ferramenta de ITSM	Permanente	N/A	<i>Commvault Backup</i>
GCLLOUD_SGI_PG_005_Auditoria Interna do SGI	Base de Conhecimento na Ferramenta de ITSM	Permanente	N/A	<i>Commvault Backup</i>
GCLLOUD_SGI_PG_008_Gestão de Não Conformidades	Base de Conhecimento na Ferramenta de ITSM	Permanente	N/A	<i>Commvault Backup</i>

Cód.: GCLLOUD_SGI_PO_001

Classificação:
PúblicoGestão do documento:
GovernançaÁrea responsável:
GovernançaPeriodicidade:
AnualVersão:
V 1.7

Plano de Auditoria Interna	Drive Compartilhado da Governança	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