ÍNDICE

1. OBJETIVO

Estabelecer os conceitos e diretrizes de segurança da informação, visando promover a disponibilidade, confidencialidade e integridade das informações necessárias para a realização dos negócios do **GRUPO QUALICORP.**

2. CAMPO DE APLICAÇÃO

Esta política aplica-se a todos os Colaboradores, prestadores de serviços, terceiros, fornecedores, parceiros comerciais e quaisquer outros profissionais que atuem para o **GRUPO QUALICORP** e que tenham acesso às informações de propriedade do **GRUPO QUALICORP.**

3. DEFINIÇÕES

3.1. Confidencialidade

Garante que a informação seja acessível somente para pessoas, processos e dispositivos autorizados. A confidencialidade se aplica aos dados armazenados, em trânsito e em processamento.

3.2. Integridade

Garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

3.3. Disponibilidade

Garante que a informação esteja disponível para as pessoas autorizadas sempre que se fizer necessária.

3.4. Violação

Considera-se violação o descumprimento de um ou mais itens desta Política.

3.5. Incidente de segurança

Ocorrência que coloca em risco a confidencialidade, integridade ou disponibilidade de um sistema de informação ou da informação que o sistema processa, armazena ou transmite. A violação e o risco iminente de violação das Políticas de Segurança também são considerados incidentes.

3.6. Segregação de funções

Princípio de segurança que requer dois ou mais indivíduos para a aprovação de uma transação, de modo a garantir que nenhum indivíduo sozinho tem informação ou privilégio suficiente para cometer fraude.

3.7. Princípio do privilégio mínimo

Princípio de segurança que consiste em conceder apenas as permissões mínimas necessárias para que o usuário possa realizar seu trabalho. Este conceito pode ser aplicado a indivíduos, programas ou processos.

3.8. LGPD

Lei Geral de Proteção de Dados Pessoais (Lei 13.709 de 14/08/2018).

4. DIRETRIZES E CRITÉRIOS

4.1. Disposições Gerais

- As informações (em formato físico ou lógico) e os ambientes tecnológicos utilizados pelos usuários são de exclusiva propriedade do **GRUPO QUALICORP**, não podendo ser interpretados como de uso pessoal.
- O uso das informações e dos sistemas de informação podem ser monitorados pela empresa e os registros obtidos durante a monitoração poderão ser utilizados para detecção de violações desta Política e das Normas

de Segurança da Informação. Essas violações podem servir de evidência para a aplicação de medidas disciplinares, processos administrativos e/ou legais.

- Todo processo, sempre que possível, durante seu ciclo de vida, deve garantir a segregação de funções.

4.2. Tratamento e Classificação da Informação

- Para assegurar a proteção adequada, as informações devem ser classificadas de acordo com o grau de confidencialidade e criticidade para o negócio do **GRUPO QUALICORP**, de acordo com a Política POL_COR_0040_CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO.
- Todas as informações devem estar adequadamente protegidas em observância às diretrizes de Segurança da Informação em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transporte e descarte.
- Toda informação que não possuir uma classificação explícita deve ser considerada implicitamente classificada como "Uso Interno".
- As informações devem ser atribuídas a um proprietário formalmente designado como responsável pela autorização de acesso às informações sob a sua responsabilidade.
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.
- Em conformidade com a Lei Geral de Proteção de Dados (LGPD), com previsão de início de vigência em agosto de 2020, dados pessoais e dados pessoais sensíveis requerem tratamento especial durante sua coleta, armazenamento, transmissão e descarte. Desta forma, é obrigatória a leitura das Políticas de Segurança especificas para a LGPD, que serão publicadas na Intranet.

4.3. Gestão de Acessos e Identidades

- O acesso aos sistemas e dados do **GRUPO QUALICORP** deve ser restrito a usuários autorizados. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado.
- Todos usuários deverão possuir credenciais de acesso (login e senha) previamente cadastradas pelo departamento de Gestão de Acessos para acessar os sistemas, dados e demais recursos tecnológicos.
- O acesso aos dados, sistemas, recursos e ambientes tecnológicos devem ser solicitado e aprovado formalmente, de forma a garantir o acesso apenas de pessoas autorizadas;
- Os acessos dos colaboradores, estagiários, prestadores de serviços e demais usuários devem ser concedidos somente com as permissões mínimas necessárias ao desempenho de suas atividades, de acordo com o princípio do privilégio mínimo.
- Os gestores são responsáveis pelas definições dos direitos de acesso dos seus subordinadas aos sistemas e dados da organização. Cabe aos gestores verificar se os usuários têm acesso compatível com suas funções e solicitar alterações, caso necessário.
- Todas as credenciais de acessos e respectivas permissões aos sistemas e dados corporativos devem ser revogadas após o término do vínculo de trabalho.

- A remoção dos acessos, tanto na infraestrutura quanto nos aplicativos, deve ser realizado de forma tempestiva. Adicionalmente, revisões periódicas serão realizadas pela área de Segurança da Informação visando minimizar a exposição de acessos indevidos.

- Todos sistemas devem possuir logs de eventos, com, no mínimo, a correta identificação do autor, a data da ocorrência e as ações realizadas.

4.4. Gestão de Incidentes de Segurança da Informação

- Compete à área de Segurança da Informação a investigação de incidentes de segurança e deliberação sobre violações desta Política.
- A área de Segurança da Informação terá acesso irrestrito aos sistemas, dados e recursos tecnológicos da empresa durante a investigação de incidentes, podendo requisitar a colaboração de outras áreas para auxiliar na investigação.
- A área de Segurança da Informação poderá acionar provedores de serviço e fornecedores externos para auxiliar na investigação e resolução de incidentes.
- Em casos de comprometimento de dados pessoais, a área de Segurança da Informação informará imediatamente o Encarregado pela Proteção de Dados Pessoais para que sejam tomadas as medidas cabíveis de acordo com a LGPD.
- A divulgação de quaisquer informações sobre incidentes de segurança deverá ser realizada somente por indivíduos autorizados pela Diretoria do **GRUPO QUALICORP**, sendo vedada a divulgação de qualquer outra forma.

4.5. Fornecedores e Prestadores de Serviços

Os contratos entre o **GRUPO QUALICORP** e empresas prestadoras de serviços com acesso às informações aos sistemas e/ou ao ambiente tecnológico do **GRUPO QUALICORP** devem conter cláusulas que garantam a confidencialidade entre as partes e que assegurem minimamente que os profissionais sob sua responsabilidade cumpram com esta Política e as Normas de Segurança da Informação.

Adicionalmente, todos os fornecedores e prestadores de serviços que tiverem acesso a dados pessoais estarão sujeitos aos requerimentos da LGPD.

4.6. Ações em Casos de Não Conformidade

- As regras que estabelecem o controle e o tratamento de situações de não conformidade, relativas à Política de Segurança da Informação e às Normas de Segurança da Informação do **GRUPO QUALICORP**, devem ser tratadas pelo Gerente de Segurança da Informação.
- O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, advertência escrita, suspensão do trabalho, rescisão do contrato de trabalho, procedimentos disciplinares e/ou processo civil ou criminal, não necessariamente nesta ordem.
- As sanções previstas devem ser aplicadas de acordo com a gravidade e a incidência da infração.

5. RESPONSABILIDADES

5.1. Funcionários, Estagiários, Prestadores de Serviços e demais Membros abrangidos por esta Política

- Cumprir fielmente as Políticas, as Normas e os procedimentos de Segurança da Informação;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pelo **GRUPO QUALICORP**;
- Assegurar que os recursos tecnológicos, as informações e sistemas a sua disposição sejam utilizados apenas para as finalidades aprovadas pelo **GRUPO QUALICORP**;
- Cumprir as leis e as normas que regulamentam a propriedade intelectual;
- Não discutir assuntos de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais, etc.), incluindo a emissão de comentários e opiniões em blogs e redes sociais;
- Não compartilhar informações do **GRUPO QUALICORP** de qualquer tipo, sem a devida autorização formal;
- Comunicar imediatamente qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos à área de Segurança da Informação.

5.2. Segurança da Informação

- Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação;
- Trabalhar na proposição, construção, análise e manutenção da Política de Segurança da Informação;
- Conduzir avaliações de segurança, podendo-se utilizar de ferramentas como testes de penetração, testes de vulnerabilidade e avaliações de risco;
- Atuar na divulgação, conscientização e treinamento de Segurança da Informação;
- Conduzir investigações em caso de incidentes de segurança e de violações desta política;
- Registrar, tratar e responder aos incidentes de Segurança da Informação;
- Estabelecer procedimentos relacionados à instrumentação da segurança da informação**.**

6. INFORMAÇÕES ADICIONAIS

Não se aplica.

7. DOCUMENTOS RELACIONADOS

- Série ISO 27001
- Normativos localizados na Qualinet - https://qualinet.qualicorp.com.br/padroes-e-projeto.
- Demais normativos de Segurança localizados no SGSI - http://colaboracao.grupo.qualicorp/si/normativos.

8. ANEXOS

Não se aplica.

D O N O	
Manoel Henrique Pinheiro Simon Gerência de Segurança da Informação	ASSINATURA

A P R O V A Ç Ã O	
Ricardo Antonio de Souza Batista Diretoria de Tecnologia da Informação	ASSINATURA

NOTA:

Esta Política tem validade de 2 anos a partir da data de sua publicação. Caso ocorra alguma alteração durante este período, compete ao Dono da Política analisar e realizar a atualização do documento.