

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



GRUPO BARCELOS
RUA ESPÍRITO SANTO, 250, 6º ANDAR – BELO HORIZONTE/MG
VER.16.0
Novembro de 2025

Sumário

1. INTRODUÇÃO	3
2. OBJETIVO	3
3. DEFINIÇÕES	4
4. PROCEDIMENTOS INTERNOS	4
4.1 Princípios da Política de Segurança da Informação	4
4.2 Divulgação e declaração de responsabilidade	6
4.3 Diretrizes da Política de Segurança da Informação	7
4.4 Monitoramento	11
5. RESPONSABILIDADES	11
5.1 Colaboradores	11
5.2 Gestores	13
5.3 Dos Proprietários de Ativos da Informação	14
5.4 Da Área de Segurança da Informação	14
5.5 Do Comitê de Segurança da Informação e LGPD	15
5.6 Da Área Jurídica	16
5.7 Da área de Recursos Humanos	16
6. OBSERVAÇÕES GERAIS	17
6.1 Penalidades	17
7. DOCUMENTAÇÃO EXTRA OBRIGATÓRIA	17
8. EVIDÊNCIA DE APROVAÇÃO	17
9. HISTÓRICO DE REVISÕES	18

1. INTRODUÇÃO

Esta Política:

- a) Tem abrangência sobre todo e qualquer conteúdo e dados produzidos, armazenados, processados ou tratados pelo GRUPO BARCELOS, sendo, portanto, considerada informação classificada do GRUPO BARCELOS, como Uso Interno.
- b) Estabelece as regras que devem ser aplicadas a todos os colaboradores (em todas as formas de relação de trabalho existentes), no que se refere à proteção da informação e uso de recursos tecnológicos do GRUPO BARCELOS, assim como a seus prestadores de serviços, parceiros e fornecedores, caso estes realizem qualquer forma de acesso ou manipulação das informações ou utilizem recursos tecnológicos de propriedade do GRUPO BARCELOS.
- c) Não prevê exceções, entretanto, caso venham a ocorrer situações não previstas por esta Política, estas deverão ser avaliadas e aprovadas pelo profissional responsável pela segurança das informações e pelo Diretor Presidente do GRUPO BARCELOS.
- d) A política foi elaborada pela área de segurança da informação e *Compliance*, em conjunto com as áreas de TI (Tecnologia da Informação), jurídica e diretoria.
- e) Deve ser revisada anualmente a partir da data de publicação pelas áreas responsáveis, sem prejuízo da realização de eventuais revisões a qualquer momento e sem aviso prévio.

2. OBJETIVO

A Política de Segurança da Informação tem por objetivo:

- a) Estabelecer diretrizes que permitam às partes interessadas do GRUPO BARCELOS seguirem padrões de comportamento desejáveis e aceitáveis sobre o tema de segurança da informação, agindo de acordo com a legalidade e de acordo com as boas práticas mundiais, visando mitigar riscos técnicos, financeiros, administrativos, jurídicos e de imagem/reputação.

- b) Nortear a definição de procedimentos específicos de Segurança da Informação, bem como a implantação de controles e processos para atendimento da mesma.
- c) Preservar as informações do GRUPO BARCELOS quanto à confidencialidade, integridade e disponibilidade.
- d) Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de consumidores e parceiros ou de qualquer outro impacto negativo ao negócio do GRUPO BARCELOS, resultante de uma ou mais falhas de segurança em seus ambientes, em especial no que diz respeito aos dados produzidos, armazenados, processados ou tratados por seus profissionais, seja em formato físico ou digital.

Esta Política é complementada por procedimentos e documentos anexos, classificados como confidenciais, e que trazem as orientações a serem seguidas na condução dos processos relacionados a esta política, e servem de referência aos profissionais encarregados da sua execução.

3. DEFINIÇÕES

As definições necessárias para o bom entendimento desta Política de Segurança da Informação são apresentadas no MANUAL DE SGSIPD que se encontra armazenado no [LINK](#).

4. PROCEDIMENTOS INTERNOS

4.1 Princípios da Política de Segurança da Informação

A informação, produzida ou recebida pelos profissionais do GRUPO BARCELOS, deverá ser utilizada com senso de responsabilidade e de modo ético e seguro, em benefício exclusivo do negócio corporativo e baseado nos seguintes princípios:

- a) **Confidencialidade:** é a garantia de que a informação não será conhecida por pessoas que não estejam autorizadas para tal. No GRUPO BARCELOS é o aspecto mais estratégico; este pilar protege o capital intelectual e, por consequência, as vantagens competitivas do GRUPO BARCELOS.

b) **Integridade:** é a garantia de que a informação armazenada ou transferida está correta e é apresentada de forma íntegra para quem a consulta. Significa que em uma comunicação, a informação não é alterada indevidamente ou corrompida no meio do trajeto entre quem emite a informação e quem a recebe. É uma característica crítica do ponto de vista operacional e indispensável, pois valida todo o processo de comunicação no GRUPO BARCELOS.

c) **Disponibilidade:** é a garantia de que a informação pode ser obtida sempre que for necessário, isto é, que esteja sempre disponível para quem precisar dela no exercício de suas funções. Quando a informação está indisponível, os processos que dela dependem ficam paralisados.

No GRUPO BARCELOS a informação é considerada como o ativo mais valioso. Sem confidencialidade perde-se vantagem competitiva, sem integridade perde-se lucratividade e sem disponibilidade perde-se a capacidade de operar. Além dos três atributos mencionados, considera-se também os seguintes:

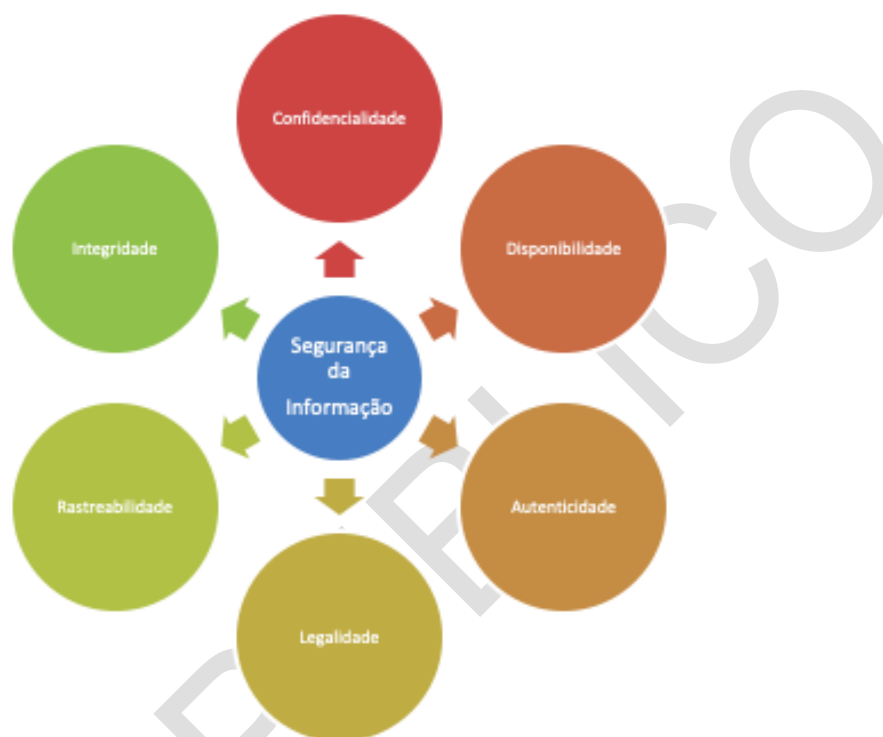
d) **Autenticidade:** é a garantia de que a informação está sendo manuseada por um usuário previamente autorizado para este tipo de atividade através da verificação da identidade digital do usuário no momento em que ele requisita um acesso – “login” em um programa ou computador. O processo de autenticação depende de um ou mais modos de autenticação: algo que o usuário conhece (senhas), algo que o usuário é (meios biométricos), algo que o usuário tem (“smart cards”, “tokens”) ou onde o usuário está (acesso somente a partir de uma máquina específica).

e) **Legalidade:** é a garantia de que a informação está gravada em conformidade com os procedimentos em vigor, ou seja, o uso da tecnologia de informática e comunicação que gerou a informação estão de acordo com as leis vigentes no local ou País.

f) **Rastreabilidade (ou Auditabilidade):** é a possibilidade de se rastrear as atualizações ocorridas em uma informação sensível para que, em caso de ocorrência de algum problema, se possa esclarecer exatamente o que aconteceu com a informação. Existem situações em que há necessidade de mecanismos capazes de rastrear o processo de volta até a origem.

Sem autenticidade, perde-se a confiança da origem fidedigna da informação, sem legalidade, há o risco de não aderência às normas regulatórias internas e externas

e sem rastreabilidade, perde-se o controle das atualizações ocorridas em dados sensíveis.



4.2 Divulgação e declaração de responsabilidade

No GRUPO BARCELOS a Política de Segurança da Informação é de conhecimento de todos os usuários e divulgada da seguinte forma:

- a) Via campanhas periódicas de Segurança da Informação; e
- b) Por meio digital, através da intranet corporativa.

A política está disponível em local de fácil acesso dos colaboradores e protegida contra alterações não autorizadas.

Todos os colaboradores, além de prestadores de serviços, parceiros e fornecedores que realizam qualquer forma de acesso ou manipulação das informações (digitais ou físicas) ou utilizem recursos tecnológicos do GRUPO BARCELOS devem aderir formalmente à “POLÍTICA DE USO DA

INTERNET, RECURSOS DE TECNOLOGIA E INFORMAÇÕES”, comprometendo-se a agir de acordo com a regras nela descrita. (Material disponível como um dos volumes da Política de Segurança da Informação).

A Política de Segurança da Informação deverá ser revisada e atualizada periodicamente, no mínimo a cada 01 (um) ano e/ou sempre que algum fato relevante ou evento ocorrer que motive a revisão antecipada da mesma, conforme análise e decisão do Comitê de Segurança da Informação e LGPD.

4.3 Diretrizes da Política de Segurança da Informação

A Segurança da Informação na organização estabelece as principais diretrizes e controles para a proteção das informações:

- a) As informações de titularidade do GRUPO BARCELOS devem ser tratadas de forma ética, sigilosa e legal e sempre se atentando aos termos acordados com colaboradores, clientes e parceiros, evitando assim o mau uso e exposição indevida de tais informações.
- b) A informação deverá ser utilizada de forma transparente, apenas para a finalidade para a qual foi designada e pelo tempo necessário para atingir a sua finalidade.
- c) Todos os usuários concordam em usar as Informações unicamente na execução de seus deveres e devidamente classificadas de acordo com a Política de Segurança da Informação.
- d) Durante sua relação de trabalho ou parceria com o GRUPO BARCELOS - e mesmo depois de findar esta - o Usuário não poderá publicar, revelar, ou de outro modo disponibilizar à qualquer terceiro, quaisquer Informações classificadas como Restritas ou Confidenciais Restritas, exceto: (i) quando expressamente autorizado por escrito pelo GRUPO BARCELOS, ou (ii) para outros colaboradores ativos que sabidamente estão autorizados a receber Informações Confidenciais e têm necessidade de conhecê-las visando sua utilização para atender às necessidades do negócio.
- e) Todos os usuários da informação têm ciência e concordam em agir com toda a diligência necessária para proteger a integridade e o sigilo das informações de propriedade do GRUPO BARCELOS, ficando vedada a subtração ou a retirada, sob qualquer forma, quaisquer materiais, exceto no que seja necessário em razão de normas ou leis em vigor.

- f) Todas as pessoas dentro das dependências físicas do GRUPO BARCELOS devem estar identificadas por crachás visíveis (ou outro meio visual de identificação). A identificação (crachá, *login*, senha, etc.) de cada colaborador é única, pessoal e intransferível, qualificando-o como responsável, civil e criminalmente, pelas ações realizadas.
- g) As senhas de acesso são de uso pessoal e intransferível e devem ser mantidas em sigilo, sendo expressamente proibido o seu compartilhamento, exceto nos casos pré-aprovados pelas áreas de Segurança da Informação.
- h) Todos os riscos identificados em relação às informações do GRUPO BARCELOS devem ser reportados para a equipe de segurança da informação através de canal específico (segurancainformacao@grupobarcelos.com.br), para que possam ser tomadas as medidas necessárias de avaliação e mitigação do risco eventualmente identificado.

Bem como todos os incidentes que afetem a segurança da informação deverão, de igual maneira, serem reportados à equipe de segurança da informação através de canal específico (segurancainformacao@grupobarcelos.com.br), que analisará o incidente e elaborará o relato.

Todo procedimento seguirá as diretrizes e normas para incidentes de segurança e, caso necessário, levará à diretoria o relato para que sejam aplicadas as devidas sanções aos envolvidos;

- i) O controle de acesso dos usuários aos ativos de informação deve ser devidamente aprovado pelo responsável pela informação, quer seja para simples consulta ou para alteração. Todas as informações relativas à solicitação, aprovação e concessão efetiva do acesso deverão ser armazenadas em um Drive seguro, com o controle de acesso configurado pelos responsáveis de cada área;
- j) O uso do e-mail corporativo disponibilizado pelo GRUPO BARCELOS é de propriedade da mesma e será permitido para usuários apenas para fins corporativos e por tempo determinado, definido pela gerência da área solicitante. Quanto à transmissão de dados, este recurso deve ser utilizado para garantir a privacidade na comunicação dos dados;
- k) Cópias de segurança de informações (*backups*), através de mídias específicas, são consideradas vitais para o sistema e para a retomada das atividades da área em caso de contingência. A política de backup é

definida e de responsabilidade do gestor da área de TI e será aprovado pelo responsável pela segurança da informação;

- l) Todos os requisitos de Segurança da Informação, incluindo a necessidade de planos de continuidade do negócio, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema. Estes requisitos devem ser justificados, acordados, documentados, implementados e testados durante a fase de execução;
- m) As regras para o desenvolvimento seguro de sistemas e softwares devem ser estabelecidas e aplicadas aos desenvolvimentos realizados dentro ou fora da organização, estando condicionadas à avaliação de adequação e aprovação do time de Segurança da Informação. No caso de desenvolvimento fora do GRUPO BARCELOS, o sistema deverá conter ferramentas que permitam auditoria de segurança quanto: autodeterminação informativa de titulares de dados, trilhas de auditoria, políticas de acesso (autenticação, autorização e rastreabilidade) e análise dos códigos fontes;
- n) A concessão de acesso remoto aos sistemas e Drives do GRUPO BARCELOS para os colaboradores, parceiros e fornecedores, deve ser autorizada formalmente. A solicitação deve ser enviada à área de TI, pelo gestor da área solicitante, ocasião em que deverá ser indicado o tipo de acesso, permissão e as informações a serem acessadas. Todo procedimento deve ser apresentado ao gestor de segurança da informação para que tenha ciência das autorizações;
- o) O uso do ambiente da internet no GRUPO BARCELOS é permitido somente para fins profissionais, onde os colaboradores devem ficar atentos aos sites que acessam e cientes que serão monitorados;
- p) Um conjunto de regras deverá ser criado para garantir a padronização das técnicas criptográficas, a aplicação adequada das mesmas e responsabilidades para manter a segurança no transporte ou armazenamento das informações, independentemente do meio utilizado. A responsabilidade em relação às regras é do gestor de TI em parceria com o gestor de segurança da informação;
- q) Os ambientes de desenvolvimento, homologação e produção devem ser segregados e devidamente controlados;
- r) Um processo de gestão de mudanças deve estar em vigor para garantir que controles e modificações nos sistemas ou recursos de processamento da informação sejam realizados com planejamento, a fim de não

ocasionar falhas operacionais ou de segurança no ambiente produtivo da organização;

- s) Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os processos nos aspectos de segurança da informação (confidencialidade, integridade e disponibilidade);
- t) Todas as informações que estiverem no meio físico (papel) deverão de igual teor serem classificadas, armazenados em local seguro, trancado, protegido contra riscos naturais, voluntários e involuntário, com controle de acesso formal por parte dos usuários visando possíveis trilhas de auditorias;
- u) Quando razões tecnológicas ou determinações superiores tornarem impossível a aplicação dos requisitos previstos nesta Política, o responsável e/ou solicitante deverá reportá-las imediatamente ao gestor de segurança da informação, para que este possibilite a adoção de medidas alternativas que mitiguem os riscos, bem como um plano de ação para corrigi-los, atenuá-los, monitorá-los ou eliminá-los;
- v) Todos os colaboradores do GRUPO BARCELOS devem passar por treinamento e conscientização sobre os procedimentos de segurança e uso correto dos ativos disponibilizados pelo GRUPO BARCELOS periodicamente, de forma a minimizar possíveis riscos de segurança, explicitar suas responsabilidades e comunicar os procedimentos para a notificação de incidentes;
- w) Todos os colaboradores do GRUPO BARCELOS devem cuidar para que os direitos de propriedade intelectual sejam preservados, tais como projetos, marcas, patentes e que o uso de produtos de softwares proprietários esteja em conformidade com a respectiva licença de uso.
- x) Todos os colaboradores do GRUPO BARCELOS devem zelar para o cumprimento da “Política de mesa limpa, tela limpa e lixo limpo”, cujo objetivo é evitar: 1) papéis e mídias de armazenamento removível em cima das mesas, 2) cestos de lixo contendo informações confidenciais legíveis, 3) telas com informações de sessões ativas ou de sessões já desativadas.

Estes cuidados são extensíveis às áreas comuns, tais como corredores, armários, áreas de armazenamento de material, salas de reunião, recintos de espera, áreas comunitárias (copa, cozinha, lazer, etc.).

4.4 Monitoramento

O GRUPO BARCELOS através de sua área de Segurança da Informação monitora e registra todo o uso das informações geradas, armazenadas ou veiculadas no GRUPO BARCELOS, a qual se reserva no direito de:

1. Implantar sistemas de monitoramento de acesso às estações de trabalho, servidores internos e externos, correio eletrônico, Internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por estes sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados.
2. Inspeccionar qualquer arquivo que esteja na rede, no disco local da estação ou qualquer outro ambiente, visando assegurar o rígido cumprimento desta Política de Segurança da Informação.
3. Instalar sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso.
4. Monitorar as instalações físicas através de câmeras.

5. RESPONSABILIDADES

5.1 Colaboradores

Todos os colaboradores do GRUPO BARCELOS:

- a) Comprometem-se a cumprir fielmente a Política, normas e procedimentos de Segurança da Informação estabelecidos neste documento, assumindo o compromisso de observá-las e aplicá-las, bem como submetendo-se às sanções previstas nas políticas internas e na legislação aplicável.
- b) Concordam que todas as operações e acessos efetuados em meios magnéticos são registrados e passíveis de verificação a qualquer momento, independentemente de aviso prévio, por se tratar de ferramentas de trabalho, não havendo que se falar em invasão de privacidade.

- c) Ficam cientes de que o GRUPO BARCELOS, conforme direito que lhe cabe, poderá realizar o monitoramento de todos os seus ambientes, sejam eles físicos, como salas de trabalho; lógicos e/ou eletrônicos, incluindo: e-mail corporativo, rede interna, Internet e Extranet e outros sistemas, armazenando os dados de acesso de cada usuário.
- d) Concordam e reconhecem que, no evento de qualquer violação dos termos e condições desta Política, estará sujeito às normas internas e à legislação em vigor. Poderá, ainda, ensejar a demissão por justa causa, nos termos do disposto no Art. 482, alínea “g”, da Consolidação das Leis do Trabalho, sem prejuízo das demais sanções legais cabíveis.
- e) Ficam cientes que, quando do término de sua relação de trabalho, ou a qualquer momento mediante requerimento do GRUPO BARCELOS, o mesmo deverá devolver todos e quaisquer materiais fornecidos, ou que contenham Informações de propriedade da mesma.
- f) Ficam cientes de que é proibida a reprodução de documentos de uso exclusivo do GRUPO BARCELOS, para quaisquer finalidades ficando tal atitude caracterizada como divulgação não autorizada de informações confidenciais e produção ilegal de provas.
- g) Devem buscar orientação junto ao gestor de segurança da informação quando houver dúvidas relacionadas à Segurança da Informação.
- h) Devem fazer o uso de senha segura, devendo alterar a mesma, conforme periodicidade determinada pelo GRUPO BARCELOS.
- i) Devem assinar a “POLÍTICA DE USO DA INTERNET, RECURSOS DE TECNOLOGIA e INFORMAÇÕES”, formalizando a ciência da Política de Segurança da Informação bem como assumindo a responsabilidade pelo seu cumprimento.
- j) Devem proteger as informações contra o acesso, modificação, divulgação ou destruição não autorizada pelo GRUPO BARCELOS.
- k) Devem assegurar que os recursos tecnológicos sejam utilizados somente para fins profissionais aprovados e de interesse do GRUPO BARCELOS.
- l) Devem comunicar imediatamente ao gestor de segurança da informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos relacionados.

5.2 Gestores

É responsabilidade de todo gestor de área do GRUPO BARCELOS:

- a) Ter conhecimento e gerenciar os acessos concedidos aos seus subordinados, sendo, portanto, responsável indireto pelo mau uso dos mesmos.
- b) Revisar periodicamente os usuários com acessos a transações críticas sob sua responsabilidade, devendo informar o RH sobre eventuais mudanças de acesso ou autorização.
- c) Ter postura exemplar em relação à Segurança da Informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.
- d) Cumprir e fazer cumprir esta Política, as Normas e Procedimentos de Segurança da Informação.
- e) Assegurar que suas equipes possuam acesso e conheçam esta Política, bem como as normas e procedimentos relacionados à segurança da informação.
- f) Atribuir na fase de contratação de terceirizados e parceiros, quando este necessitar ter contato com informações da companhia, a inserção de cláusula de responsabilidade, ciência da Política de Segurança da Informação e confidencialidade, exigindo o repasse das obrigações a seus empregados responsáveis pela prestação de serviços dentro do GRUPO BARCELOS.
- g) Especificar e solicitar previamente permissão de acesso, elencando os ativos de informação para os colaboradores em geral que não sejam contratados.
- h) Adaptar às Normas, Processos, Procedimentos e Sistemas sob sua responsabilidade para atender a esta Política de Segurança da Informação.
- i) Comunicar imediatamente ao gestor de segurança da informação, através de Canal específico (segurancainformacao@grupobarcelos.com.br), eventuais violações da Segurança da Informação, que acionará e trabalhará em conjunto com a equipe de Segurança da Informação.

5.3 Dos Proprietários de Ativos da Informação

O Proprietário da informação pode ser um diretor, gerente ou coordenador de uma determinada área ou projeto, o qual será o responsável pela manutenção, revisão, cancelamento e classificação (em conjunto com os seus subordinados) das informações que serão inseridas nos sistemas e drives do GRUPO BARCELOS, bem como configurar o nível de acesso às mesmas, de acordo com necessidade do uso de cada usuário.

Uma outra responsabilidade do proprietário é a segregação de função.

5.4 Da Área de Segurança da Informação

Cabe ao time de Segurança de Informação do GRUPO BARCELOS:

- a) Submeter ao Comitê de Segurança da Informação e LGPD as versões da Política e das normas de Segurança da Informação, e após a aprovação, publicar e promover as mesmas na intranet do GRUPO BARCELOS.
- b) Propor e apoiar iniciativas que visem à segurança dos ativos de informação do GRUPO BARCELOS.
- c) Promover, junto à área de RH, conscientização dos colaboradores e parceiros em relação à relevância da Segurança da Informação para o negócio do GRUPO BARCELOS, através de campanhas, palestras, treinamentos e outros meios.
- d) Analisar criticamente incidentes, com apoio do time de TI, se necessário;
- e) Manter comunicação efetiva com o Comitê de Segurança da Informação e LGPD, com o objetivo de mantê-los adequadamente informados sobre assuntos relacionados ao tema, que afetem ou tenham potencial para afetar o GRUPO BARCELOS.
- f) Receber as denúncias sobre violações da Política e das Normas, após concretização das investigações realizadas, devendo promover a tratativa das informações, identificação do plano de ação, mitigação de risco, acionamento do Comitê de Segurança da Informação e LGPD e aplicação da sanção cabível (Penalidades).

Cabe ao time de TI do GRUPO BARCELOS:

- a) Realizar a gestão do uso de tecnologias necessárias ao bom andamento dos negócios do GRUPO BARCELOS, incluindo ações preventivas e tratamento de incidentes, a fim de promover maior nível de segurança da informação.
- b) Realizar as ações direcionadas às questões técnicas.
- c) Propor as metodologias e processos específicos para a Segurança da Informação, em conjunto ao gestor de Segurança de Informação, como por exemplo, Avaliação de Risco.
- d) Apoiar a avaliação e a adequação de controles específicos de Segurança da Informação para novos sistemas ou serviços, em conjunto com o time de Segurança de Informação.
- e) Tomar medidas imediatas de forma a remediar eventual violação verificada pela área e cessar de imediato o risco ao GRUPO BARCELOS, informando imediatamente ao gestor de Segurança de Informação sobre a violação e medidas implementadas.

5.5 Do Comitê de Segurança da Informação e LGPD

O Comitê de Segurança da Informação e LGPD é formado por gestores das principais áreas do GRUPO BARCELOS, que devem cumprir as seguintes responsabilidades dentro da organização.

- a) Garantir a disponibilidade de recursos para todas as ações de Segurança da Informação.
- b) Manter o foco e promover a Segurança da Informação no GRUPO BARCELOS, aprovando políticas que reflitam o seu papel acima descrito mediante aprovação de material submetido pelo gestor de Segurança de Informação.
- c) Garantir que riscos à Segurança de Informação sejam identificados, avaliados, categorizados e gerenciados pelo gestor de Segurança de Informação responsável para tanto.

- d) Aprovar ações custo-efetivo para realizar a gestão dos riscos e monitorar a sua implantação.
- e) Dar direcionamento, revisar e atualizar a estratégia de Segurança da Informação garantindo que sua Política, MANUAL DE SGSIPD sejam adequadamente atualizados e continuamente pertinentes ao cenário do GRUPO BARCELOS.
- f) Garantir que treinamento e conscientização sobre Segurança da Informação seja fornecido para colaboradores e, quando pertinente, a terceiros, fornecedores e clientes.

5.6 Da Área Jurídica

Cabe à Área Jurídica do GRUPO BARCELOS:

- a) Orientar para a melhor forma de coleta e preservação de prova eletrônica, com o objetivo de manter sua eficácia para uso em juízo, quando necessário; e
- b) Elaborar e revisar documentos jurídicos relacionados à Segurança da Informação, principalmente à proteção dos dados definidos pela LGPD e assegurar cláusulas que mitiguem os riscos jurídicos;

5.7 Da área de Recursos Humanos

A área de RH deve atribuir, na fase de contratação dos colaboradores e formalizar nos contratos individuais de trabalho, a responsabilidade quanto ao cumprimento da Política de Segurança da Informação.

Cabe à Área RH:

1. Colher a assinatura da “POLÍTICA DE USO DA INTERNET, RECURSOS DE TECNOLOGIA e INFORMAÇÕES” dos colaboradores já contratados e em novos processos de contratação, bem como efetuar o arquivamento da mesma;
2. Fomentar treinamentos a área de segurança da informação (LGPD), bem como administrar os certificados concedidos aos colaboradores do GRUPO BARCELOS;

3. Comunicar à área de TI e Segurança da Informação formal e prontamente toda e qualquer alteração no quadro funcional da instituição, contratações, demissões, alterações de cargos, funções, entre outros necessários, em prazo mínimo, a fim de evitar acessos não autorizados e/ou desnecessários.

6. OBSERVAÇÕES GERAIS

6.1 Penalidades

Quando entender necessário e relevante, o time de Segurança de Informação submeterá as infrações à Política de Segurança da Informação e às Normas de Segurança da Informação à diretoria, assim como o resultado da apuração validado através do comitê de segurança da informação e LGPD e demais áreas pertinentes, conforme a Política de Apuração de Denúncias do GRUPO BARCELOS.

Ao colaborador suspeito de cometer violações à Política e Normas de Segurança da Informação, deverá ser assegurado tratamento justo e correto, sendo que toda e qualquer medida resultante de sua infração, deverá ser aplicada com proporcionalidade à ocorrência com base na Norma de Infrações e Penalidades.

O GRUPO BARCELOS se exime de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de punir os infratores, analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios e adotar as medidas legais cabíveis.

7. DOCUMENTAÇÃO EXTRA OBRIGATÓRIA

- a) POLÍTICA DE USO DA INTERNET, RECURSOS DE TECNOLOGIA e INFORMAÇÕES
- b) Manual SGSIPD
- c) Código de Conduta e ética

8. EVIDÊNCIA DE APROVAÇÃO

É de ciência e acordo entre as áreas envolvidas que esta Política entre em vigor:

NOME	CARGO	ASSINATURA
Claudio Roberto Magalhães Pessoa	DPO	
Renato Georges Ferreira	Gerente de TI	
Servio Tulio de Barcelos	CEO	
Julio Cesar Nogueira Duarte	Superintendente Administrativo e Financeiro	

9. HISTÓRICO DE REVISÕES

Revisão	Data da Revisão	Revisor	Inserção/alteração/Remoção
1	23/12/2020	Matheus Nunes	Criação do documento
2	02/02/2022	Fábio Sena	Controle criptográfico
3	09/02/2022	Fábio Sena	Metas de SI
4	18/02/2022	Fábio Sena	Metas de SI pela direção
5	08/03/2022	Fábio Sena	Responsabilidades da direção, Gestão de não conformidades
6	14/03/2022	Fábio Sena	Atribuições do comitê
7	16/03/2022	Fábio Sena	Descarte de mídia
8	29/03/2022	Fábio Sena	Trilha zero
9	27/04/2022	Fábio Sena	Processo disciplinar, Segregação de funções
10	13/05/2022	Fábio Sena	Histórico de versões
11	24/05/2022	Fábio Sena	Criptografia para transferência de dados
12	02/06/2023	Fabio Sena	Atualização das responsabilidades dos membros do comitê de SI e revisão do documento
13	14/07/2023	Fabio Sena	Item 10.3.1 Inclusão de parâmetros de senha
14	14/08/2024	Fábio Sema	Revisão do documento. Atualização do item 10.3.3
15	26/09/2024	Fábio Sena	Atualização item 9.10.3
16	15/11/2025	Renato George	Revisão do documento