Norma de Segurança da Informação

SUMÁRIO

1. OBJETIVO

A informação é um dos ativos mais valiosos da Companhia. Assim, esta norma tem como objetivo estabelecer diretrizes, responsabilidades e princípios para proteção da informação na empresa.

2. APLICAÇÃO

Aplica-se a todos os colaboradores e prestadores com acesso a informações da Companhia.

3. DEFINIÇÕES

- **Ativo de Informação**: Qualquer dado, sistema, serviço ou recurso com valor para a organização.
- **Auditoria**: Verificação sistemática da conformidade com políticas, procedimentos e controles.
- **Boas Práticas de Segurança da Informação**: Recomendações amplamente aceitas para proteger informações e sistemas.
- **Ciclo de Vida da Informação**: Conjunto de fases pelas quais a informação passa, da criação ao descarte.
- **Classificação da Informação**: Categorização da informação conforme sua sensibilidade e impacto em caso de vazamento.
- **Código de Conduta e Ética**: Documento com os padrões de comportamento esperados dos colaboradores.
- **Comitê de Segurança da Informação**: Grupo que avalia, propõe e decide ações relacionadas à segurança da informação.
- **Confidencialidade**: Garantia de acesso à informação apenas por pessoas autorizadas.
- **Criptografia**: Técnica para codificar dados e impedir acessos não autorizados.
- **DPO (*Data Protection Officer*)**: Encarregado pelo tratamento de dados pessoais e conformidade com a LGPD.
- **Disponibilidade**: Garantia de que a informação estará acessível quando necessário.

- **Identidade**: Conjunto de atributos que identificam unicamente um usuário ou sistema.
- **Incidente de Segurança da Informação**: Evento que compromete (ou pode comprometer) a confidencialidade, integridade ou disponibilidade da informação.
- **Integridade**: Garantia de que a informação não foi alterada ou corrompida de forma indevida.
- **LGPD (Lei Geral de Proteção de Dados)**: Lei brasileira que regula o tratamento de dados pessoais.
- **Recurso Corporativo**: Ferramentas, dispositivos, sistemas e infraestrutura disponibilizados pela empresa.
- **Revisão de Acesso**: Verificação periódica das permissões de usuários para garantir adequação.
- **Segregação de Funções**: Separação entre as atividades de autorização, execução e controle.
- **Segurança da Informação**: Responsável pela revisão e atualização periódica dos procedimentos relacionados à classificação e proteção das informações da empresa.
- **Vulnerabilidade**: Fragilidade que pode ser explorada para comprometer a segurança de um sistema ou informação.

4. RESPONSABILIDADES

4.1. Todos os colaboradores e prestadores de serviços

- **Colaboradores e prestadores**: Devem proteger as informações com as quais lidam, seguindo as boas práticas de segurança da informação.
- **Gestores**: Devem garantir o cumprimento das diretrizes de segurança da informação por suas equipes.
- **Alta administração**: Deve apoiar e promover o cumprimento desta norma e documentos relacionados.

4.2. Área de Segurança da Informação, Riscos e Conformidade (SRM)

- Promover a conscientização de segurança da informação a todos os colaboradores da empresa.
- Identificar e avaliar riscos de segurança e implementar medidas de controle.
- Implementar, monitorar e controlar as diretrizes de segurança.
- Gerenciar incidentes de segurança e vulnerabilidades.
- Apoiar as áreas de negócio a conduzir suas atividades de maneira segura.
- Garantir que os ativos de informação estejam acessíveis a quem de direito e protegidos contra acessos e alterações não autorizadas.

4.3. Área de Infraestrutura

- Garantir que a infraestrutura tecnológica da organização esteja disponível, íntegra, eficiente e em conformidade com as diretrizes.
- Assegurar a operação segura e confiável de servidores, redes e dispositivos de infraestrutura.
- Implementar políticas para garantir que sistemas e softwares recebam atualizações de segurança em tempo hábil.
- Garantir cópia de segurança de dados para recuperação em caso de perda ou incidente.

4.4. Área de Suporte Aplicações/Serviços TI

- Implementar e supervisionar controles de acesso aos sistemas geridos por Digital.
- Proteger os dados conforme as melhores práticas de segurança.
- Monitorar continuamente o desempenho e a segurança das aplicações.
- Garantir que as aplicações estejam protegidas de ameaças e corrigir vulnerabilidades de segurança.
- Gerenciar os processos de gestão de mudanças.

4.5. Encarregado de Dados (DPO)

- Garantir a conformidade com as leis de privacidade, tratando os dados pessoais de maneira segura e ética.
- Proteger os direitos dos titulares de dados, minimizar riscos de incidentes de segurança relacionados a dados pessoais e promover uma cultura de privacidade na organização.

5. DIRETRIZES

5.1. Classificação e Tratamento da Informação

A informação deve ser protegida com recursos corporativos durante todo o seu ciclo de vida, baseado nos seguintes princípios:

- **Confidencialidade**: Garantia que a informação é disponibilizada ou divulgada a indivíduos, entidades ou processos autorizados.
- **Integridade**: Garantia 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.
- **Disponibilidade**: Garantia que a informação esteja disponível sempre que necessário.
- **Autenticidade**: Garantia que a credencial de acesso a informação sempre é verificada.
- **Irretratabilidade**: Garantia de provar o que foi feito, quem fez e quando fez, impossibilitando a negação de suas ações, também conhecido como “não repúdio”.

Toda informação deve ser classificada com base nos critérios da empresa e na legislação vigente, conforme detalhado no Procedimento de Classificação das Informações.
O uso de recursos não corporativos para tratar informações da empresa é proibido, salvo autorização formal por processo corporativo.
As informações geradas por colaboradores e prestadores de serviço no exercício de suas funções são propriedade da empresa, que pode monitorar e utilizá-las conforme necessário.

5.2. Controle de Acesso e Identidade

O acesso a sistemas e informações seguirá o princípio do menor privilégio, garantindo que usuários tenham apenas as permissões necessárias para desempenhar suas funções.

Senhas devem ser fortes, alteradas periodicamente e protegidas por autenticação multifatorial quando aplicável.

O controle de acesso deve assegurar que permissões sejam concedidas apenas a quem necessita, restringindo o acesso indevido.

Todo o acesso deve ser identificável e rastreável, garantindo a auditoria das ações realizadas. Cada usuário deve possuir uma identificação única, pessoal e intransferível.

Senhas de credenciais de autenticação devem ser mantidas em sigilo. O seu compartilhamento é proibido.

Os acessos devem ser revisados periodicamente e sempre que houver mudança de função, realocação ou desligamento de colaboradores e prestadores de serviço.

As regras e o processo para concessão, bloqueio e revogação de acessos estão definidos no Procedimento de Controle de Acesso Lógico.

5.3. Gestão de Incidentes

Incidentes de segurança devem ser identificados, reportados e tratados com agilidade, conforme o processo de resposta a incidentes. A Companhia mantém um plano de ação para mitigar impactos e assegurar a continuidade dos negócios.

5.4. Recursos de Tecnologia

Os recursos de tecnologia disponibilizados pela empresa — incluindo, mas não se limitando a computadores, redes corporativas, correio eletrônico, acesso à internet, smartphones e softwares — devem ser utilizados para fins profissionais. O uso moderado para fins pessoais é permitido, desde que seja breve, não afete a produtividade e não comprometa a segurança da empresa.

5.5. Registro e Monitoramento de Uso da Informação

A empresa se reserva no direito de monitorar e controlar o uso da informação de acordo com as diretrizes internas e requisitos legais.

Serão realizadas auditorias periódicas e monitoramento contínuo para garantir o cumprimento desta norma e identificar potenciais vulnerabilidades.

5.6. Partes Externas

Todos os contratos com prestadores de serviços que tenham acesso a informações da empresa devem conter cláusulas de confidencialidade e privacidade.

5.7. Segregação de Função

Todos os processos de negócio devem obedecer ao princípio da segregação de funções, que estabelece a separação entre as atividades de execução, aprovação e controle.
Nenhum colaborador deve possuir atribuições que violem esse princípio.

5.8. Treinamento e Conscientização

Todos os colaboradores e, quando aplicável, os prestadores de serviços devem receber treinamentos adequados e atualizações periódicas sobre as políticas e os procedimentos de Segurança da Informação.

5.9. Conformidade

Todos os processos da empresa devem atender integralmente às diretrizes internas, exigências legais e regulatórias de segurança da informação e privacidade de dados.

5.10. Aceitação da Norma de Segurança da Informação

É obrigatório que todos os colaboradores reconheçam formalmente e comprometam-se com às disposições desta norma e suas atualizações.

5.11. Violação à Norma de Segurança da Informação

Violações desta norma ou de documentos complementares estarão sujeitas a sanções definidas pelo Comitê de Segurança da Informação, composto por representantes de Segurança da Informação, Compliance, Jurídico e Gente & Gestão (Recursos Humanos).

Colaboradores devem relatar imediatamente qualquer violação desta norma. A omissão também será considerada uma violação.

O tratamento das violações segue o Procedimento de Tratamento de Incidentes de Segurança da Informação, que define as etapas de contenção, análise e classificação de gravidade.

Casos que envolvam dados pessoais ou dados pessoais sensíveis serão encaminhados ao time do Encarregado de Dados (DPO).

Casos com impacto significativo, reincidência ou indícios de má-fé serão escalonados ao Comitê de Segurança da Informação, responsável pela análise e aplicação das sanções cabíveis.

5.12. Considerações Finais

Este documento substitui a anterior Política de Segurança da Informação, mantendo sua validade e aplicabilidade nos termos previamente estabelecidos, inclusive em documentos contratuais, normativos ou operacionais que façam referência à versão anterior.

6. PENALIDADES

O descumprimento deste documento está sujeito à aplicação de medidas disciplinares, contratuais e legais apropriadas, conforme e a gravidade da violação. Essas medidas serão implementadas de acordo com o Código de Conduta e Ética e diretrizes de Tratamento de Incidentes de Compliance, demais documentos e legislação pertinentes.

7. CASOS OMISSOS

Todo assunto não previsto no presente documento deve ser encaminhado para avaliação e aprovação da Diretoria Executiva da área emitente e Diretoria Executiva Jurídica. Quando a área solicitante reportar para Diretoria Executiva Jurídica, deverá constar também a aprovação da Diretoria Executiva Financeira.

As evidências da aprovação devem ser arquivadas pela área emitente deste documento para fins de futuras auditorias.

8. REFERÊNCIAS

8.1. Documentos Externos Relacionados

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD)
- Lei nº 12.965/2014 – Marco Civil da Internet

8.2. Documentos Internos Relacionados

- Norma de Boas Práticas Para Contratação de Novas Soluções Tecnológicas
- Procedimento de Classificação das Informações
- Procedimento Controle de Acesso Lógico
- Procedimento Disponibilização de Informações de Colaboradores ou Ex Colaboradores
- Procedimento Segurança Física de Sistemas Computadorizados
- Procedimento para Uso de Plataformas de Internet e Comunicação
- Procedimento de Tratamento de Incidente de Segurança da Informação
- Procedimento de Uso Recursos de Tecnologia da Informação
- Procedimento de Registro e Monitoramento de Eventos de Segurança Da Informação
- Procedimento de Gestão de Conta de Usuário Genérico
- Procedimento de Resposta a Incidentes de Cibersegurança
- Procedimento de Acesso a Mídias Removíveis

9. ANEXOS

Não aplicável.

10. ELABORAÇÃO E VALIDAÇÃO

Área Emitente	Elaborado por	Cargo
Segurança da Informação e Riscos	Rosemery Maximino De Oliveira	COORD SEGUR INFORMACAO

Data	Validado por	Cargo
03/06/2025	Alinne Marciano Batista	ANL CONTROLES INTERNOS SR
03/06/2025	Claudio Roberto Gomes Bernardo	GTE SEGUR INFORMACAO SR
18/06/2025	Rafael Vito Batista	DIR EXEC OPERACOES
18/06/2025	Tiago Roberto Goncalves	GTE OPERACOES E SERVICOS G&G SR
22/06/2025	Livia Abilio Giovanetti Shimizu	GTE COMPLIANCE E GOVERNANCA SR
04/07/2025	Alexander dos Santos	COORD JURIDICO
16/07/2025	Alinne Marciano Batista	ANL CONTROLES INTERNOS SR
-	-	-
-	-	-

Validação Complementar

Segue informações da validação complementar do documento: data, nome e cargo dos aprovadores. Se a validação complementar não for aplicável, nenhuma informação será registrada abaixo.

-