Algar SEMPRE JUNTO	**PO.DSI.02.21 - SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA**	
POLÍTICA	**Data de Criação/Alteração:** 15/03/2024	**Versão:** 21
DSI	**Criado/Alterado por:** Segurança da Informação	**Validade:** 3 anos

1. OBJETIVO

Prover diretrizes, orientação, apoio e melhorias contínua dos serviços para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações aplicáveis, de forma a preservar a confidencialidade, integridade e disponibilidade das informações da Algar, manter os fatores de risco dentro do limite de probabilidade aceitável pela organização e garantir a aderência dos associados e terceiros aos requisitos de segurança da informação.

Esta Política de Segurança da Informação e Cibernética foi construída a partir das estratégias do negócio, requisitos contratuais e legislação vigente e é aplicável a todas as unidades da Algar, independente de regional, incluindo o Data Center.

2. PÚBLICO-ALVO

As diretrizes aqui estabelecidas devem ser seguidas por todos os associados, prestadores de serviços, fornecedores, estagiários e parceiros que utilizam de alguma forma os processos, instalações e informações da Algar, assim como por seus clientes, quando aplicável, para garantia do serviço.

3. DOCUMENTOS REFERÊNCIAIS

- Código de Conduta Algar;
- Política Corporativa de Gestão de Consequências;
- Política Uso Aceitável de Inteligência Artificial (IA) Generativa;
- Leis nº 12.735 e 12.737, de 30 de novembro de 2012, Leis de Delitos Informáticos;
- Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais;
- Resolução nº 740, 21 de dezembro de 2020 - Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações;
- Lei nº12.965, de 23 de abril de 2014 – Marco Civil da Internet;
- Decreto nº 8.771, de 11 de maio de 2016 – Regulamenta o Marco Civil da Internet;
- Norma NBR ISO/IEC 27001:2022 – Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação – Requisitos;

- Norma NBR ISO/IEC 27002:2022 – Segurança da Informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação;
- Norma ISO 27701 – Tecnologia da Informação – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão de privacidade da informação;
- Norma NBR 16167 – Segurança da Informação – Diretrizes para classificação, rotulação e tratamento e gestão da informação;
- Norma ISO/IEC 27014– Tecnologia da Informação – Técnicas de Segurança – Governança de Segurança da Informação;
- COBIT 5 – Control Objectives for Information and Related Technology. ISACA, ITGI, 2012.
- Política de Governança em Privacidade e Proteção de Dados Pessoais da Algar;
- OWASP - Open Worldwide Application Security Project.

4. ÁREA RESPONSÁVEL PELO DOCUMENTO

Diretoria de Segurança da Informação

5. PAPÉIS E RESPONSABILIDADES

5.1 As principais áreas envolvidas nos processos e procedimentos de Segurança da Informação na Algar são as seguintes:

5.1.1 Presidente (CEO): Assegurar às partes interessadas que riscos de segurança da informação são gerenciados, e afirmar seu compromisso e da sua equipe para com a segurança da informação, leis e regulamentações aplicáveis ao negócio, a partir desta Política de Segurança da Informação e Cibernética;

5.1.2 Vice-presidência InfraCo: Ter conhecimento dos objetivos e diretrizes descritas na Política de Segurança da Informação e Cibernética e nas demais políticas e normas da empresa, e garantir a aderência das equipes durante o período em que estiverem prestando serviços à empresa. Também é de sua responsabilidade a implementação de medidas de segurança da informação, visando mitigar os riscos, sempre com o envolvimento da área de Gestão de Segurança da Informação;

5.1.3 Vice-presidência de Tecnologia: Ter conhecimento dos objetivos e diretrizes descritas na Política de Segurança da Informação e Cibernética e nas demais políticas e normas da empresa, e garantir a aderência das equipes durante o período em que estiverem prestando serviços à empresa. Também é de sua responsabilidade a implementação de medidas de segurança da informação, visando mitigar os riscos, sempre com o envolvimento da área de Gestão de Segurança da Informação;

5.1.4 Vice-presidência de Talentos Humanos: Responsável por apoiar a disseminação e comunicação de políticas, normas e treinamentos para todos os associados em relação à Segurança da Informação, assim como no apoio à aplicação da gestão disciplinar por consequência do descumprimento das diretrizes de segurança pelos associados;

5.1.5 Diretoria de Segurança da Informação (DSI): Ter conhecimento dos objetivos e diretrizes descritas na Política de Segurança da Informação e Cibernética e nas demais políticas e normas da empresa, e garantir a aderência das equipes durante o período em que estiverem prestando serviços à empresa. Também é de sua responsabilidade a definição das políticas e normas de apoio a esta política, de medidas de segurança, como o monitoramento de ativos e processos de tecnologia, assim como o gerenciamento destes controles a fim de mitigar quaisquer eventos quanto a incidentes e ameaças ou quanto ao uso indevido dos ativos e recursos da Algar;

5.1.6 Área de Compliance: Realizar a análise de eficácia dos controles associados aos riscos de Segurança da Informação, enquanto papel da 2a linha de gestão com objetivo de estabelecer níveis de controles adequados para mitigação destes e assegurar o reporte nos fóruns apropriados.

5.1.7 Escritório de Privacidade: A equipe de privacidade tem como objetivos principais, mas não se limitando, a gerenciar e garantir a aplicação do programa de privacidade e proteção de dados pessoais. Orientar e avaliar os riscos relacionados à Privacidade, além disso, tem, entre outras, a atribuição de revisar e elaborar políticas sobre o tema, de gerenciar os inventários e registros de tratamentos e de operacionalizar os controles e políticas adotados;

5.1.8 Encarregado de dados / DPO: É a pessoa indicada pela alta administração para representar a Algar atuando como um canal de comunicação entre a empresa, os Titulares de Dados e a Autoridade Nacional de Proteção de Dados (ANPD). Sendo responsável pela gestão da proteção de dados dentro da organização, garantindo o cumprimento da LGPD e demais legislações de privacidade, promovendo a segurança das informações de titulares de dados pessoais relativos aos negócios da Algar.

5.1.9 Associados Algar e Terceiros: Cabe a todo associado ou terceiro a serviço a responsabilidade de conhecer e cumprir as diretrizes de Segurança da Informação e Cibernética estabelecidas pela Algar. O descumprimento das diretrizes sujeita à aplicação da gestão disciplinar ou ação judicial, quando for o caso.

5.1.10 As demais funções e responsabilidades envolvidas na administração e controle da Segurança da Informação estão formalizadas por meio do documento específico "Funções e Responsabilidades pela Segurança da Informação" disponível para consulta na biblioteca de documentos da Algar.

6. DEFINIÇÕES

6.1 Segurança da Informação: É a preservação da confidencialidade, integridade e disponibilidade da informação. Ou seja, são os esforços contínuos para a proteção dos ativos de informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco à empresa, maximizar o retorno sobre os investimentos e as oportunidades de negócios. É obtida a partir da implementação de controles adequados incluindo políticas, processos, procedimentos, estruturas organizacionais e tecnologia para garantir que os objetivos do negócio e de segurança da empresa sejam atendidos;

6.2 Segurança Cibernética: Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade e a confidencialidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;

6.3 Confidencialidade: Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento dos não autorizados;

6.4 Integridade: Garantia de que as informações estejam fidedignas e completas para o uso em relação à última alteração desejada durante o seu ciclo de vida;

6.5 Disponibilidade: Garantia de que as informações e os Recursos de TIC (item 6.15) estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso;

6.6 Legalidade: Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do Ordenamento Jurídico em vigor;

6.7 Autenticidade: Garantia de que a informação foi criada, editada ou emitida por quem se disse ter sido, sendo capaz de gerar evidências não repudiáveis em relação ao criador, editor ou emissor;

6.8 Informação: É o conjunto de dados agrupados de forma lógica que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato;

6.9 Privacidade: Controle da exposição, distribuição e uso de informações pessoais disponibilizadas pelo próprio dono da informação;

6.10 *Security by Design:* Refere-se à segurança de processos e sistemas, englobando melhores práticas e padrões de segurança aplicados desde a concepção e desenho, seguindo as melhores práticas de mercado.

6.11 *Privacy by Design:* Significa privacidade desde a concepção, executado pela área de privacidade, assegurando que processos e sistemas sejam projetados de tal forma que a coleta e o tratamento (incluindo o uso, divulgação, retenção, transmissão e descarte) estejam limitados ao que é necessário para o propósito identificado;

6.12 Terceiro: Remete a todos aqueles que possuem atuação na Algar, mas não fazem parte do seu quadro de associados. Terceiros pode-se referir à: parceiros de negócio, fornecedores, prestadores de serviços e/ou ativos etc.;

6.13 Ativo de Informação: É qualquer coisa que tenha valor para a Algar e precisa ser adequadamente protegido;

6.14 Inventário de informações e outros ativos associados: Identifica as informações da empresa e outros ativos associados, a fim de preservar a sua segurança da informação e atribuir a propriedade adequada;

6.15 Recursos de TIC (Tecnologia da Informação e Comunicações): São todos os recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação. Entre os tipos de recursos podemos destacar: computadores de mesa ou portáteis, smartphones, tablets, pen drive, discos externos, mídias, impressoras, scanners, entre outros. Sempre que mencionados de forma a não identificar seu possuidor ou proprietário, os Recursos de TIC compreenderão tanto os pertencentes à Algar quanto aos particulares em proveito corporativo;

6.16 Violação: Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos da Algar;

6.17 Incidente de Segurança da Informação: É a perda de um ou mais princípios da segurança da informação, ou seja, uma quebra na confidencialidade, integridade e disponibilidade das informações. Pode ser considerada também como uma ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede que indica possível violação à Política de Segurança da Informação e Cibernética ou documentos complementares, falha de controles ou situação previamente desconhecida e que possa ser relevante à segurança da informação.

7. DIRETRIZES GERAIS

7.1 Esta Política de Segurança da Informação e Cibernética tem como intenções:

7.1.1 Preservar e proteger as informações da Algar e os Recursos de TIC que as contêm, ou que estejam sob sua responsabilidade, dos diversos tipos de ameaça em todo o seu ciclo de vida, contidas em qualquer suporte ou formato;

7.1.2 Estabelecer as responsabilidades dos associados, prestadores de serviços, fornecedores, estagiários, parceiros e clientes que utilizam de alguma forma informações da Algar em relação à segurança da informação e comunicação, reforçando a cultura interna e priorizando as ações necessárias conforme a criticidade do ativo;

7.1.3 Definir as melhores práticas, padrões, recomendações e uso dos Recursos de TIC por meio de suas diretrizes e normas complementares, resguardando a segurança das informações da Algar e utilizando controles de acordo com os níveis de riscos envolvidos;

7.1.4 Prevenir e reduzir impactos gerados por incidentes de segurança da informação e de privacidade de dados, assegurando a confidencialidade, integridade e disponibilidade no desenvolvimento das atividades profissionais.

7.1.5 Para suportar a implementação dos requisitos de segurança da informação e determinações da presente política, os documentos complementares devem estar disponíveis na biblioteca de documentos da Algar;

7.1.6 A Política de Segurança da Informação e Cibernética e seus documentos complementares devem ser interpretados de forma restritiva, ou seja, as atividades que não estão tratadas na normativa só devem ser realizadas após análise prévia da equipe de Gestão de Segurança da Informação e formal autorização do executivo responsável pelo associado ou diretor/comitê executivo da Algar, conforme o aplicável;

7.1.7 A Política de Segurança da Informação e Cibernética deve estar disponível a todos os associados, clientes, fornecedores e parceiros, visando dar sua publicidade para todos que se relacionam profissionalmente com a Algar;

7.1.8 A Política de Segurança da Informação e Cibernética deve ser revisada a cada 3 (três) anos pela Diretoria de Segurança da Informação, em conjunto com REDIR e aprovação pelo Conselho de Administração, ou sempre que alterações significativas no SGSI (Sistema de Gestão de Segurança da Informação) ocorrerem. A análise crítica da Política de Segurança da Informação e Cibernética deve ser realizada a cada 12 (doze) meses;

7.1.9 Esta política deve ser disponibilizada no site da Algar, demonstrando transparência quanto aos compromissos da empresa com as demandas de segurança cibernética e da informação, mas resguardando-se de informações classificadas e sensíveis ao negócio;

7.1.10 A Algar, por meio da Diretoria da Segurança da Informação, deve promover um "Programa de Conscientização" para disseminação da cultura de Segurança da Informação junto aos seus associados e prestadores de serviço.

7.2 SEGURANÇA DA INFORMAÇÃO PARA PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

7.2.1 Na Algar, todos os associados devem respeitar a privacidade. Assim, deve garantir a disponibilidade, integridade, confidencialidade dos dados pessoais em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte, por meio de diretrizes específicas ao tema.

7.3 ESTRUTURA PARA A SEGURANÇA DA INFORMAÇÃO

7.3.1 Pessoas

7.3.1.1 Associados Algar

- Devem ter conhecimento das políticas vigentes na empresa, em especial a Política de Segurança da Informação e Cibernética e o Código de Conduta Algar, inclusive em regime de trabalho remoto;

- Devem realizar os Treinamentos de Conscientização em Segurança da Informação, devendo atuar em conformidade com os ensinamentos;

- Os associados que atuam diretamente nos processos e procedimentos da estrutura de segurança da informação mencionados nesta política devem possuir conhecimento específico para execução de suas atividades, devendo a Algar implementar diretrizes para identificação das necessidades de capacitação de seu quadro técnico e disponibilizar programas de treinamento, capacitação e/ou certificação;

- Devem assinar o Termo de Compromisso e Responsabilidade e Acordo de Confidencialidade no ato de sua admissão, ou sempre que solicitado pela empresa.

7.3.2 Gestão de Terceiros

7.3.2.1 Devem estar aderentes ao documento específico de gestão de riscos de segurança de terceiros, considerando a definição de diretrizes para validação da capacidade técnica, aderência aos requisitos de segurança cibernética e da informação descritos nesta política e a realização de auditorias ou apresentação de relatórios equivalentes, por órgão independente, que possam validar a maturidade das práticas e ambiente cibernéticos do terceiro;

7.3.2.2 Ao final do vínculo contratual, o responsável pelo contrato dos prestadores de serviço da Algar deve garantir que as credenciais de autenticação utilizadas durante os trabalhos sejam devidamente desabilitadas.

7.3.3 Gestão de Ativos

7.3.3.1 A Algar deve implementar um documento formalizado com as diretrizes para a identificação e definição dos controles adequados para a proteção e segurança dos ativos da empresa.

7.3.4 Acesso à Rede Corporativa

7.3.4.1 Os acessos à rede corporativa da Algar devem ser controlados e monitorados, conforme processos e diretrizes definidos em documento específico;

7.3.4.2 Na rede corporativa, não é permitida a utilização de computadores pessoais, salvo mediante aprovação executiva e aprovação da equipe de gestão de segurança da informação, estando condicionados às políticas e demais diretrizes de segurança, e podem ser desconectados a qualquer momento, caso seja necessário;

7.3.4.3 A Algar deve documentar e implementar mecanismos que possam limitar e monitorar os *sites* que os associados e terceiros têm acesso em seus ativos na rede corporativa, mitigando os potenciais impactos que acesso a sites e serviços *web* possam ter no ambiente da empresa, mas sem prejudicar as atividades de cada profissional.

7.3.5 Acesso Lógico

7.3.5.1 Os processos de gestão de acessos lógicos, como a concessão, transferência, revalidação e revogação de acessos ao ambiente da Algar, devem estar descritos em documento específico;

7.3.5.2 As credenciais de acesso aos ambientes tecnológicos da Algar devem ser únicas para cada associado ou terceiro e intransferíveis;

7.3.5.3 As permissões de acesso associadas às credenciais dos associados e terceiros devem ser concedidas somente para os ativos TIC, funcionalidades e informações estritamente necessárias para o desempenho de suas atividades;

7.3.5.4 As senhas utilizadas pelas credenciais devem possuir tamanho, complexidade e tempo de utilização definidos por documento específico de controle de acesso lógico.

7.3.6 Segurança e Acesso Físico

7.3.6.1 A segurança física determina o perímetro e controle relacionado à concessão de acesso físico, de acordo com a criticidade das informações tratadas nestes ambientes, hospedagem de dispositivos críticos e documentos sigilosos, sendo que as diretrizes devem estar descritas em documento específico;

7.3.6.2 A Algar deve se certificar que as barreiras de controle de acesso implementadas sejam apropriadas para cada perímetro de segurança identificado, considerando os critérios do item anterior;

7.3.6.3 Requisitos específicos para acesso de visitantes, fornecedores e quaisquer outros terceiros aos ambientes considerados críticos devem ser descritos em documento específico de segurança e acesso físico;

7.3.6.4 Os acessos aos ambientes físicos considerados críticos devem ser registrados, monitorados e revisados, sendo documentado os procedimentos a serem realizados para adoção destes controles;

7.3.6.5 As localidades onde os ativos TIC estejam hospedados devem possuir robustez e equipamentos de segurança que possam proteger os ativos de ameaças externas e do meio ambiente (ex.: sub e sobretensão, invasões, alagamentos,

incêndios, desabamentos etc.) e que tais mecanismos sejam compatíveis com a criticidade dos ativos.

7.3.7 Proteção e Classificação da Informação

7.3.7.1 O acesso às informações da Algar e/ou seus clientes em seu ambiente empresarial e computacional é restrito e será disponibilizado somente ao perfil de pessoas formalmente autorizadas, considerando o princípio do mínimo privilégio aos acessos concedidos no ambiente da Algar;

7.3.7.2 A Algar deverá definir, em documento específico, as diretrizes acerca da classificação e rotulagem das informações conforme sua criticidade, independentemente de sua natureza (física ou digital), e os meios de controles aplicáveis a cada nível de informação, tanto em repouso quanto em trânsito;

7.3.7.3 Informações acerca de dados pessoais sensíveis e demais informações consideradas críticas ao negócio devem possuir mecanismos de mascaramento de dados que irão atuar como camadas de proteção adicionais às mencionadas anteriormente, garantindo a anonimização ou pseudonimização das informações.

7.3.8 Prevenção de Vazamento de Dados

7.3.8.1 A Algar deverá, por meio de documento específico, implementar procedimentos para que os ativos de informação em seu ambiente tecnológico sejam identificados, monitorados e protegidos contra vazamento e divulgação indevida que possam impactar a empresa;

7.3.8.2 Os procedimentos documentados devem considerar todos os ativos que processam informações no ambiente da Algar, seja com dados em repouso ou em trânsito;

7.3.8.3 Este procedimento deve ser implementado alinhado aos requisitos de classificação e rótulo de informações, onde serão definidos, implementados e monitorados os controles aplicáveis para cada tipo de informação e seu respectivo nível de criticidade.

7.3.9 Exclusão de Informações

7.3.9.1 Os responsáveis pelas informações devem documentar e implementar os procedimentos para que as informações armazenadas em suas bases de dados, em ambientes em nuvem, mídias removíveis ou quaisquer outros ambientes ou meios venham ser descartadas do ambiente tecnológico da empresa, de forma segura e irreversível;

7.3.9.2 Os procedimentos a serem documentados devem definir prazos para exclusão dos ativos de informação, considerando o tempo mínimo necessário por órgãos reguladores, legislações aplicáveis ou por necessidade de procedimentos de auditoria.

7.3.10 Aquisição, Desenvolvimento Seguro e Manutenção de Sistemas de Tecnologia

- Requisitos de segurança de sistemas devem ser identificados e acordados antes da aquisição conforme diretrizes definidas em documento específico.

- A Algar deve definir as diretrizes para que todo sistema adquirido ou desenvolvido, seja por associado ou por terceiro, siga um ciclo de vida de desenvolvimento seguro de software, respeitando os princípios do *security by design* e *privacy by design* e dos testes em código;

- Os responsáveis pelo sistema de tecnologia da informação devem definir diretrizes, em documento específico, para validação da capacidade técnica do terceiro em prestar manutenção aos sistemas e garantir a aderência à política de segurança cibernética e da informação da empresa.

7.3.11 Gestão de Configurações Seguras

- A Algar deve documentar e formalizar diretrizes para definição, implementação, monitoramento e revisão periódica, ao menos uma vez por ano, das linhas de base de configurações seguras em seus ativos e recursos TIC;

- Em complemento às diretrizes acima, a Algar deve definir processos de instrução de trabalho para implementação das linhas de base de configurações de cada ativo e Recurso TIC em seu ambiente tecnológico.

7.3.12 Gestão de Incidentes de Segurança da Informação

- Um processo de gestão de incidentes para identificação, registro, tratamento e resposta a incidentes deve ser definido em documento específico;

- Um Plano de Resposta a Incidentes deve ser implementado na Algar, considerando o mapeamento dos principais incidentes com potencial de ocorrência no ambiente da empresa, e definida as diretrizes de resolução em todas as etapas de resolução de um plano de resposta;

- O Plano de Resposta a Incidentes deve ser revisado anualmente, e os resultados dos testes, assim como resultados de resposta à incidentes reais, devem ser documentados e utilizados como insumos para que ajustes no plano, quando necessário, sejam realizados.

7.3.13 Gestão de Continuidade de Negócios

- Os responsáveis pelos processos de negócios críticos devem definir, implementar e testar anualmente um plano de continuidade de negócios que viabilize a recuperação desses processos e de toda a operação em cenários diversos e de crise;

- Todos os procedimentos de salvaguarda de dados e de redundância e capacidade dos ativos TIC que suportam a continuidade de negócios devem ser revisados, minimamente,

na periodicidade de revisão do Plano de Continuidade de Negócios, a fim de garantir sua eficácia e eficiência, quando necessário;

- Todo procedimento de revisão ou de execução do Plano de Continuidade de Negócios deve ser documentado para que os procedimentos realizados sejam considerados para melhoria contínua do referido plano.

7.3.14 Gestão de Riscos de Segurança Cibernética e da Informação

- A Algar deve atender às diretrizes de riscos corporativos e adicionalmente gerenciar os riscos internos referentes às suas disciplinas e as especificidades de riscos de segurança cibernética e da informação e seus respectivos controles e medidas mitigadoras que possam minimizar ou erradicar estes riscos;

- Os processos de gestão de riscos cibernéticos devem considerar a avaliação dos limites de riscos do ambiente da Algar, utilizando frameworks, referências de mercado específicas para a avaliação de riscos de Segurança da Informação e Cibernética. Este gerenciamento de riscos internos deve ser realizado de forma complementar ao gerenciamento de riscos corporativos.

- Os processos de gestão de riscos cibernéticos devem estar documentados e formalizados, e suas diretrizes devem estar alinhadas com esta política, além da política corporativa de gestão de riscos.

7.3.15 Gestão de Vulnerabilidades

- A Algar deve documentar e implementar processos de gestão de vulnerabilidades técnicas, determinando as responsabilidades, diretrizes para identificação, análise e classificação da criticidade e até sua contenção/erradicação;

- Todos os procedimentos executados para mitigação ou erradicação de uma vulnerabilidade devem ser documentados para fins de auditoria e melhoria dos processos;

- O processo de gestão de vulnerabilidades técnicas deve ser avaliado e revisado, ao menos, anualmente;

- O processo de gestão de vulnerabilidades deve ser implementado considerando um fluxo paralelo de *input* dos resultados provenientes do procedimento de inteligência de ameaças;

- Os procedimentos de gestão de vulnerabilidades documentados devem considerar os requisitos dos procedimentos de gestão de ativos, de incidentes, de mudanças e de gestão de riscos cibernéticos e de segurança da informação, a fim de que sejam executados de forma consistente e integrada com os outros normativos.

7.3.16 Inteligência de Ameaças

- A Algar deve documentar as diretrizes e procedimentos de buscas acerca de informações sobre o *brand* e os ativos e informações da empresa para identificação de ameaças e/ou oportunidades de melhoria no ambiente da empresa;

- O procedimento deve considerar a integração, das ameaças e oportunidades de melhoria identificadas, ao processo de gestão de vulnerabilidades implementado na empresa.

7.3.17 Treinamento e Conscientização

- A Algar deve documentar e formalizar processos para implementação, comunicação, execução e acompanhamento dos treinamentos e campanhas sobre conscientização em segurança da informação.

7.3.18 Comunicação Corporativa

- A Algar deve documentar e formalizar diretrizes para implementação dos processos de comunicação corporativa, considerando atender as necessidades das partes interessadas, tanto internas quanto externas, implementando canais apropriados e observando os diferentes cenários aplicáveis ao procedimento.

7.3.19 Compartilhamento Seguro de Dados

- A Algar deve documentar e formalizar diretrizes para o compartilhamento de dados e informações com as partes interessadas de maneira segura, considerando os requisitos do regulador e das legislações de privacidade e proteção de dados aplicáveis ao negócio da empresa;

- A Algar deve-se resguardar, nos processos de compartilhamento de dados e informações, de quaisquer informações pessoais ou sensíveis ao seu negócio.

7.4 AUDITORIAS E MONITORAMENTO

7.4.1 A Algar reserva-se o direito de monitorar e manter registros de todos os tipos de acesso aos seus sistemas ou a sistemas de terceiros a partir do ambiente e/ou equipamentos da empresa e/ou de terceiros durante todo o período de prestação de serviços. Estes registros são utilizados para análises estatísticas e para verificação pontual em casos relacionados com incidentes de segurança;

7.4.2 A Algar reserva-se também no direito de executar auditorias internas para a verificação do atendimento dos itens que compõem esta política e demais normas, sem prévio aviso;

7.4.3 Havendo descumprimento das recomendações da presente política e normas da empresa, e nos casos de não conformidade em auditorias internas, medidas disciplinares podem ser tomadas conforme Política de Gestão de Consequências do Grupo Algar, disponível para conhecimento na biblioteca de documentos da Algar Holding;

7.4.4 Cada caso identificado deve ser avaliado pela equipe de Gestão de Segurança da Informação, em conjunto com a equipe de Talentos Humanos para tomada de decisão.

7.5 USO DE TECNOLOGIAS EMERGENTES

7.5.1 A Algar deve definir diretrizes para que tecnologias emergentes sejam utilizadas nos processos de negócio da empresa, respeitando as normativas específicas relacionadas à segurança da informação quanto ao uso responsável de ativos, aos critérios definidos nos procedimentos de aquisição e desenvolvimento de sistemas e aos processos de classificação e proteção de dados;

7.5.2 Toda e qualquer nova tecnologia emergente que for utilizada na Algar, deve seguir todas as diretrizes dessa política e deve ser avaliada pela área de Segurança da Informação e ter documentada a avaliação de riscos de acordo com as diretrizes de avaliação de Riscos Cibernéticos e de Segurança;

7.5.3 Conectividade 5G

7.5.3.1 A Algar deve implementar e documentar medidas de segurança em suas redes 5G, sejam públicas ou privadas, considerando o aumento da superfície de ataque ao ambiente da empresa inerentes da tecnologia por conta de sua alta velocidade e baixa latência;

7.5.3.2 Procedimentos específicos para controle de acesso granular às diferentes partes e camadas dos serviços oferecidos pelas redes 5G devem ser documentados e implementados;

7.5.3.3 A Algar deve documentar e implementar procedimentos para testes de resiliência e segurança nos ativos TIC que fazem parte da infraestrutura 5G.

7.5.4 Internet das Coisas (IoT)

7.5.4.1 A Algar deve implementar e documentar procedimentos para proteção de seus dispositivos IoT, considerando aqueles desenvolvidos com viés de segurança em seu design, disponibilidade de atualizações e monitoramento regulares;

7.5.4.2 Dispositivos IoT devem ser considerados *Zero Trust* no ambiente da Algar. Com isso, documentos específicos para segmentação e isolamento, monitoramento do tráfego e do comportamento dos ativos e testes de segurança e avaliações regulares devem ser implementados e revisados;

7.5.4.3 Procedimentos específicos para gestão do ciclo de vida, padrões de desenvolvimento e de configuração segura dos ativos IoT devem ser desenvolvidos, de acordo com as diretrizes definidas nesta política.

7.5.5 Computação de Borda de Acesso Múltiplo (MEC)

7.5.5.1 Com a disponibilidade de serviços de múltiplos acessos tanto nas redes 5G quanto nas demais redes, a Algar deve implementar e documentar mecanismos de segurança que venham proteger os ativos e recursos TIC implementados na borda, garantindo que tanto os dados, quanto ativos e serviços sejam processados e armazenados de forma segura.

7.5.6 Uso de Serviços em Nuvem

7.5.6.1 A Algar deve documentar e implementar os requisitos da aquisição, uso, gerenciamento e saída dos serviços em nuvem;

7.5.6.2 Procedimentos específicos para controle do acesso, segregação e monitoramento dos ambientes e dados hospedados em nuvem devem ser

documentados e implementados, considerando as diretrizes já definidas para estes temas para os ativos da Algar;

7.5.6.3 Os procedimentos para uso dos serviços em nuvem devem abordar as configurações do ambiente em nuvem para o tratamento de dados seguro e acesso somente por pessoal autorizado.

7.5.7 Uso de Inteligência Artificial/IA Generativa

7.5.7.1 A Algar deve definir, em documento específico, os pré-requisitos para uso de modelos de inteligência artificial para que as bases de dados utilizadas para consulta e treino do modelo sejam aplicáveis única e exclusivamente aos processos de negócio da empresa, livre de quaisquer vieses e que sejam validadas periodicamente por procedimentos de auditoria regulares;

7.5.7.2 O uso de inteligência artificial em processos de negócio da Algar deve estar em conformidade com as regulamentações de proteção de dados vigentes e aplicáveis ao negócio, e sua utilização também deve ser refletida nos códigos de conduta da empresa;

7.5.7.3 Campanhas de treinamento e conscientização do uso seguro de inteligência artificial devem ser adotadas pela Algar;

7.5.7.4 Controles devem ser implementados para utilização de dados de alta classificação, em especial dados pessoais sensíveis, nas bases de dados utilizadas para treinamento dos modelos.

7.6 SANÇÕES E PENALIDADES

7.6.1 A Algar não considera que a conduta que viole esta Norma esteja dentro do curso e âmbito das atividades de um associado, parceiro ou prestador de serviço, ou como consequência direta da execução de suas funções. Consequentemente, na medida do permitido por lei, a empresa se reserva o direito de não defender e/ou pagar quaisquer custos ou danos que resultem.

7.7 DISPOSIÇÕES FINAIS

7.7.1 O presente documento deve ser lido e interpretado sob o amparo das leis locais, no idioma português;

7.7.2 Para conhecer mais sobre os processos de Segurança da Informação da Algar, entre em contato com: seginfo@algartelecom.com.br;

7.7.3 Para comunicação de incidentes de Segurança da Informação e Cibernética, entre em contato com: cybersecurity@algartelecom.com.br;

8. DESCUMPRIMENTO DO DOCUMENTO

8.1 Qualquer dúvida sobre o processo ou cumprimento das regras contidas neste documento, entre em contato com a área responsável ou superior imediato, permitindo ajustes e melhoria contínua. Ou caso ache necessário, temos o nosso Canal de Ética, para recebimento de denúncias por descumprimento das diretrizes do Código de Conduta e demais documentos internos, que após as devidas apurações, poderão ensejar a aplicação de medidas disciplinares, através da Subcomissão de Integridade, previstas na Política Corporativa de Gestão de consequências, bem como sanções legais cabíveis.

9. CANAL DE ÉTICA

9.1 Um canal para associados, fornecedores ou demais público de interesses para recebimento de denúncias no caso de descumprimentos do Código de Conduta, documentos normativos e legislações aplicáveis;

9.2 Os relatos registrados são tratados com absoluto sigilo, imparcialidade. Todos os registros são analisados de forma criteriosa e responsável, contribuindo para a gestão transparente e um ambiente confiável.

- Site: https://www.algar.com.br/canaldeetica
- Telefone: 0800 034 2525
- E-mail: canaldeetica@algar.com.br

10.VIGÊNCIA

10.1 Este documento possui validade de 3 anos, contados a partir da data de sua aprovação

11.ANEXOS

11.1 Atas de reunião da Redir e CA.