Política de Segurança da Informação

Adotado pelo Conselho de Administração na sua reunião de 28 de outubro de 2025

INDICE

1 INTRODUO

Atualmente, as tecnologias da informação enfrentam um número crescente de ameaças, o que requer um esforço constante para se adaptar e gerenciar os riscos que elas introduzem. O objetivo da Política de Segurança da Informação (doravante "Política") é adotar um conjunto de medidas para preservar a confidencialidade, integridade e disponibilidade das informações, e estabelecer os requisitos de alto nível necessários para proteger as informações, equipamentos e serviços tecnológicos, que suportam os processos empresariais das empresas que compõem o Grupo Amper (doravante "Grupo Amper"). Esta Política de Segurança da Informação é a pedra angular do Corpo de Normas de Segurança do Grupo Amper. O Corpo de Normas de Segurança (CNS) é um conjunto de documentos em diferentes níveis que compõem os requisitos, diretrizes e protocolos de segurança que o Grupo Amper deve seguir. O CNS deve ser desenvolvido por cada sociedade do Grupo Amper mediante um conjunto de documentos (normas de uso, normas regulatórias, procedimentos, manuais, guias, boas práticas, etc.) de modo que cubram todos os aspectos apresentados na Política, atingindo o nível do processo operacional.

1.1 OBJETIVO

O objetivo principal desta Política é definir os princípios e regras básicas para a gestão da segurança da informação. O objetivo final é garantir que as empresas do Grupo Amper garantam a segurança da informação e minimizem os riscos não financeiros decorrentes do impacto causado por uma gestão ineficaz da informação.

1.2 Alcance

A Política é aplicável a todo o Grupo Amper, que deve cumprir este requisito mínimo sem prejuízo da possibilidade de implementar políticas mais restritivas. Além disso, as filiais deverão adaptar e desenvolver esta Política nas suas empresas e deverão informar a matriz do Grupo Amper do seu cumprimento com esta Política. O escopo desta Política abrange todas as informações das empresas do Grupo Amper, independentemente de como são processadas, quem as acessa, o suporte que as contém ou onde se encontram, sejam elas impressas ou armazenadas eletronicamente. A Política estará disponível no site corporativo

da Amper www.grupoamper.com e em um repositório comum da Amper, para que seja acessível a todas as pessoas do Grupo Amper.

1.3 ADAPTAO E DESENVOLVIMENTO POR PARTE DAS FINALIDADES DE POLTICA

Esta política de segurança da informação deve ser adaptada e desenvolvida por cada sociedade do Grupo Amper. Cada sociedade decidirá como a Política se adapta às suas operações mediante documentação específica (seu Organismo de Normas de Segurança, CNS), que sempre estará alinhada com as diretrizes estabelecidas neste documento.

2 PRINCPIOS DE POLTICA DE INFORMAO

Esta Política responde às recomendações das melhores práticas de segurança da informação estabelecidas na Norma Internacional ISO/IEC 27001 e no Esquema Nacional de Segurança, bem como ao cumprimento da legislação vigente sobre a proteção de dados pessoais e as regulamentações que possam afetar o Grupo Amper no âmbito da segurança da informação.

Além disso, o Grupo Amper estabelece os seguintes princípios básicos como diretrizes fundamentais para a segurança da informação que devem ser sempre consideradas em qualquer ação relacionada com o processamento de informação:

- Alcance estratégico: A segurança da informação deve contar com o compromisso e apoio dos níveis de gestão das sociedades do Grupo Amper para coordenar e integrar-se com o resto das iniciativas estratégicas a fim de formar um quadro de trabalho coerente e eficaz.
- Segurança integral A segurança da informação deve ser considerada parte da operação habitual, estando presente e aplicada durante todo o processo de concepção, desenvolvimento e manutenção de sistemas de informação.
- Gestão de riscos: A análise e a gestão de riscos serão uma parte essencial do processo de segurança da informação. A gestão de riscos permitirá manter um ambiente controlado, minimizando os riscos a níveis aceitáveis. A redução desses níveis será alcançada através da implantação de medidas de segurança, que equilibrarão a natureza dos dados e o processamento, o impacto e a probabilidade dos riscos a que estão expostos, e a eficácia e custo das medidas de segurança.
- Proporcionalidade: O estabelecimento de medidas de proteção, detecção e recuperação deve ser proporcional aos riscos potenciais e à criticidade e valor das informações e serviços em questão.
- Melhoria contínua: As medidas de segurança serão regularmente reavaliadas e atualizadas para adaptar sua eficácia à evolução constante dos riscos e sistemas de proteção. A segurança da informação será atendida, revisada e auditada por pessoal qualificado.
- Segurança por defeito: Os sistemas devem ser projetados e configurados de forma a garantir um grau suficiente de segurança por defeito.

O Grupo Amper considera que as funções de Segurança da Informação devem ser integradas em todos os níveis do seu pessoal. Como a Segurança da Informação é da responsabilidade de todo o pessoal do Grupo Amper, esta Política deve ser conhecida, compreendida e assumida por todos os seus funcionários. Para alcançar os objetivos desta Política, o Grupo Amper deverá estabelecer uma estratégia preventiva para analisar os riscos que podem afetá-lo, identificá-los, introduzir controles para sua mitigação e estabelecer procedimentos regulares para sua reavaliação. No decurso deste ciclo de melhoria contínua, o Grupo Amper manterá a definição tanto do nível de risco residual aceito como dos seus limiares de tolerância.

3 COMPROMISSO DA DIREO

A Direção do Grupo Amper, consciente da importância da segurança da informação para alcançar com êxito os seus objetivos de negócio, compromete-se a:

- Promover na organização as funções e responsabilidades no âmbito da segurança da informação.
- Disponibilizar os recursos adequados para atingir os objetivos de segurança da informação.
- Impulsionar a divulgação e a sensibilização para a Política de Segurança da Informação entre os colaboradores do Grupo Amper.
- Exigir o cumprimento da Política, da legislação em vigor e dos requisitos das entidades reguladoras no âmbito da segurança da informação.
- Considerar os riscos de segurança da informação na tomada de decisões.

4 PAPÉIS E RESPONSABILIDADES

O Grupo Amper compromete-se a garantir a segurança de todos os ativos sob a sua responsabilidade mediante as medidas necessárias, assegurando sempre o cumprimento das diferentes normativas e leis aplicáveis.

Nas empresas do Grupo Amper, deve ser designada uma figura responsável por definir, implementar e supervisionar as medidas de cibersegurança e segurança da informação. Será sua responsabilidade desenvolver e manter a Política, garantindo que seja adequada e oportuna à medida que evoluem tanto a sociedade Amper Group da qual você é responsável como a normativa vigente.

5 GESTO DA SEGURANA DE RECURSOS HUMANOS

O Departamento de Recursos Humanos será responsável por sua gestão tendo em conta os critérios de segurança estabelecidos na Política de Segurança da Informação, que é um ponto chave para garantir o cumprimento. Os requisitos estabelecidos nesta Política devem ser salvaguardados em todos os momentos, incluindo a fase pré-recrutamento, a fase de recrutamento e a eliminação progressiva dos contratos de funcionários.

5.1 FORMAO E CONSCINCIA

O Grupo Amper deve garantir que todo o pessoal receba um nível adequado de formação e conscientização no domínio da segurança da informação, especialmente no domínio da confidencialidade e da prevenção de fugas de informação. Os funcionários também serão informados das atualizações das políticas e procedimentos de segurança em que são afetados e das ameaças existentes para garantir a conformidade. Por outro lado, os funcionários têm a obrigação de agir com diligência em relação às informações, garantindo que essas informações não caiam nas mãos de funcionários ou terceiros não autorizados.

5.2 POLTICA DE TABELAS LIMITADAS

São estabelecidos os seguintes requisitos com o objetivo de manter a segurança do trabalho: A sessão da equipe deve ser bloqueada quando o empregado sai do posto, tanto por meios manuais (bloqueio por parte do usuário) Isso inclui a necessidade de que qualquer documento ou suporte informativo seja mantido fora da vista, mantendo aqueles classificados como confidenciais ou secretos sob confinamento (ver parágrafo 20.1 "Anexo: Níveis de classificação").

6 GESTO DE ATIVOS

Os ativos de informação necessários para o fornecimento dos processos empresariais do Grupo Amper devem ser identificados e inventariados. Além disso, o inventário de ativos deve ser mantido atualizado. 7Classificação de informaçõesClassificação de ativos de acordo com o tipo de informações a serem processadas, de acordo com o parágrafo 7 "Classificação de informações". Ao longo de todo o ciclo de vida, deve ser designada uma pessoa responsável por realizar a gestão própria dos ativos de informação. O controlador deve manter um registro formal dos usuários com acesso autorizado a esse ativo. Além disso, para cada ativo ou elemento de informação haverá um responsável ou proprietário, que será responsável por garantir que o ativo esteja inventário, devidamente classificado e protegido adequadamente. As configurações de ativos devem ser atualizadas regularmente para permitir o rastreamento de ativos e facilitar a atualização correta das informações.

6.1 BYOD OU GESTO DE DISPOSITIVOS PESSOAIS

O Grupo Amper adota a política conhecida como BYOD (Traga seu próprio dispositivo), que permite aos funcionários usar seus dispositivos móveis pessoais ou recursos para acessar recursos ou recursos do Grupo Aper. Além disso, os usuários devem ter em conta uma série de requisitos estabelecidos nesta Política: As mesmas medidas e configurações de

segurança devem ser aplicadas aos dispositivos BYOD que tratam as informações, bem como a outros dispositivos do Grupo Amper. O usuário será responsável pelo equipamento BYOD. Os usuários devem manter atualizado o dispositivo BYOD pessoal onde tratam qualquer tipo de informação do Grupo Amper. Os funcionários devem ser autorizados pelo seu gerente de área a usar dispositivos BYOD. Qualquer incidente que possa afetar a confidencialidade, integridade ou disponibilidade desses dispositivos deve ser comunicado ao gerente de segurança.

6.2 INFORMAES SOBRE A GESTO DO CICLO DE VIDA

O Grupo Amper deve gerenciar adequadamente o ciclo de vida da informação, evitando usos incorretos durante qualquer

O ciclo de vida de um ativo de informação consiste nas seguintes fases:

1. Criação ou coleta: esta fase trata os registros em seu ponto de origem. Isso pode incluir a sua criação por um membro do Grupo Amper ou o recebimento de informações de uma fonte externa. Inclui correspondência, formulários, relatórios, desenhos, entrada/saída informática ou outras fontes.
2. Distribuição: é o processo de gestão da informação uma vez que foi criado ou recebido. Isso inclui tanto a distribuição interna como externa, uma vez que as informações que saem do Grupo Amper se tornam um registro de uma transação com terceiros.
3. Uso ou acesso: ocorre depois que a informação é distribuída internamente, e pode gerar decisões de negócios, novas informações ou servir para outros fins. Detalha o conjunto de usuários autorizados pelo Grupo Amper para acessar as informações.
4. Armazenamento: é o processo de organizar a informação em uma sequência predefinida e criar um sistema de gestão para assegurar a sua utilidade dentro do Grupo Amper. Sem um método de armazenamento para informar, a recuperação e o uso seriam quase impossíveis.
5. Destruição: estabelece as práticas para a eliminação de informações que cumpriram os períodos de retenção definidos e as informações que deixaram de ser úteis para o Grupo Amper. Os períodos de retenção das informações devem basear-se nos requisitos regulatórios, legais e legais que afetam o Grupo Amper. As necessidades empresariais também devem ser levadas em consideração. Se nenhum destes requisitos exigir que as informações sejam conservadas, devem ser eliminadas por meios que garantam a sua confidencialidade durante o processo de destruição.

O Grupo Amper identificará medidas de segurança de acordo com esta Política para garantir a gestão adequada do ciclo de vida dos ativos.

6.3 GESTO DE CPIOS DE SEGURANA

Devem ser realizadas cópias de segurança e revistas periodicamente. Para fazer isso, os backups de aplicativos, arquivos e bancos de dados devem ser feitos pelo menos uma vez por semana, a menos que nenhuma atualização tenha sido feita durante esse período. Quando apropriado, uma maior frequência de backup pode ser estabelecida se as

informações a serem protegidas tiverem um alto impacto para o Grupo Amper e/ou um alto nível de transação. Como regra geral, a frequência com que os backups serão realizados será determinada de acordo com a sensibilidade das aplicações ou dados, de acordo com os critérios de classificação para a informação declarados no Anexo "Níveis de classificação". Os backups devem receber as mesmas proteções de segurança que os dados originais, garantindo sua correta preservação, bem como controles de acesso adequados.

Como regra geral e sempre que possível, as informações nos backups devem ser criptografadas. Este requisito será obrigatório para certos tipos de informações confidenciais. Devem ser realizados testes de restauração de backups disponíveis e processos de restauração definidos para garantir o correto funcionamento dos processos. Estes serão realizados regularmente e deverão ser documentados. Será estabelecido um período de conservação de cópias de segurança até à sua destruição após o final do período de existência. Os backups de arquivos mestres, aplicativos e arquivos de informações devem estar localizados em locais seguros com acesso restrito. Além disso, os backups serão de preferência localizados em um centro diferente do que os gerou ou na nuvem. Você deve garantir que haja um backup adicional de informações sensíveis protegidas contra escrita, para garantir sua integridade diante da necessidade de recuperação de possíveis incidentes de segurança associados, por exemplo, com ransomware.

7 CLASSIFICAO DA INFORMAO

Deve ser definido um modelo de classificação para a informação que permita o conhecimento e implementação das medidas técnicas e organizacionais necessárias para manter sua disponibilidade, confidencialidade e integridade. O modelo de classificação integrará os requisitos e condições estabelecidos nesta seção da Política. O modelo de classificação terá uma pessoa responsável por atualizá-lo quando for considerado apropriado e de informá-lo a todos os funcionários do Grupo Amper.

7.1 Classificação de informações

Amper classificará as informações de acordo com o suporte em que se utilize:

- Meios lógicos: informações utilizadas por meios de escritório, e-mail ou sistemas de informação desenvolvidos para medir ou adquiridos de um terceiro.
- Meios físicos: informação em papel, suportes magnéticos

7.2 NÍVEIS DE CLASSIFICAÇÃO

Em função da sensibilidade da informação, o Grupo Amper deverá classificar a informação em cinco níveis. Consulte a definição detalhada no Anexo **“Níveis de Classificação”**:

- Uso público
- Difusão limitada

- Informação confidencial
- **Informação reservada**
- **Informação secreta**

7.3 GESTO DE INFORMAES PRIVILEGIADAS

As informações consideradas confidenciais, confidenciais ou secretas devem ser tratadas com especial cuidado. Medidas de segurança extraordinárias ou adicionais devem ser definidas para o tratamento adequado de informações internas.

7.4 ROTULAGEM DE INFORMAES

O Grupo Amper deve rotular por métodos manuais ou, na medida do possível, automatizados para facilitar o tratamento adequado das medidas de segurança que aplicam em cada caso. Os documentos ou materiais, bem como os anexos, cópias, traduções ou extractos dos mesmos, devem ser rotulados de acordo com os níveis de classificação das informações definidas no subparágrafo anterior, com excepção das informações consideradas de "Uso público". Um processo ou procedimento deve ser definido para a rotulagem das informações de acordo com os seguintes requisitos:

- Classificar a rotulagem das informações pode refletir o esquema de classificação das informações adotadas.
- Garantir que as etiquetas sejam facilmente reconhecíveis entre todos os funcionários.
- Orientar os funcionários sobre onde e como as etiquetas serão colocadas ou usadas, dependendo do processo de acesso às informações ou dos recursos que as suportam.

Deve-se prestar especial atenção e tratar com o máximo cuidado a rotulagem dos ativos físicos que contêm informações secretas ou secretas para evitar que seu roubo seja facilmente identificável. Deverão ser estabelecidas medidas técnicas, se necessário, e viáveis para a rotulagem automática das informações suportadas nos meios digitais. O Grupo Amper deve garantir a formação e formação de todos os seus funcionários na rotulagem da informação, bem como formar e formar especificamente os funcionários que tratam a informação em nível secreto ou reservado.

7.5 MANIPULAO DE INFORMAES

O Grupo Amper será responsável por desenvolver e implementar um conjunto adequado de procedimentos para o correto manuseio das informações.

7.6 PRIVACIDADE DA INFORMAO

O Grupo Amper deve garantir a privacidade dos dados pessoais para proteger os direitos fundamentais das pessoas físicas, em particular o seu direito à honra, à privacidade pessoal

e familiar e à imagem, estabelecendo medidas para regular o tratamento de dados. O Grupo Amper deve cumprir com a legislação vigente relativa à proteção dos dados pessoais segundo a jurisdição em que esteja constituída e opere (de forma ilustrativa, Lei Orgânica 3/2018, de 5 de dezembro, sobre a Proteção de Dados e Garantias de Direitos Digitais no caso da Espanha) e deve incluir as medidas necessárias para cumprir com a normativa. Devem ser implementadas medidas adequadas para garantir a privacidade das informações em todas as fases do seu ciclo de vida (de acordo com a Seção 6.2 Gestão do Ciclo de Vida da Informação).

8 PREVENO DE FONTES DE INFORMAO

A fuga de informação consiste numa saída não controlada de informação (intencional ou não intencional), que faz com que esta chegue a pessoas não autorizadas ou que o seu proprietário perca o controlo sobre o acesso à mesma por parte de terceiros.

Deverão ser analisados os vetores de fuga de informação, em função das condições e da operacionalidade de trabalho de cada sociedade do Grupo Amper. Para tal, deverão ser identificados os ativos cuja fuga represente maior risco para cada sociedade, com base na criticidade do ativo e no nível de classificação da informação. Além disso, deverão ser identificadas as possíveis vias de roubo, perda ou fuga de cada um dos ativos nas diferentes fases do seu ciclo de vida.

O Grupo Amper deverá definir procedimentos para evitar situações que possam provocar a perda de informação, bem como procedimentos de atuação caso seja comunicada uma fuga de informação.

Deverá ser assegurada a formação e capacitação de todos os colaboradores relativamente às boas práticas de prevenção de fugas de informação. Em especial, deverão ser considerados, pelo menos, os seguintes aspetos:

- Processo de gestão de dispositivos de elevada criticidade identificados;
- Utilização adequada de dispositivos amovíveis, tais como USB, CD/DVD ou semelhantes;
- Utilização do correio eletrónico;
- Transmissão oral de informação;
- Impressão de documentação;
- Saída de documentação das instalações;
- Utilização de dispositivos móveis;
- Utilização da Internet;

- Secretárias limpas e organizadas (ver secção 5.2 – Política de Secretárias Limpas);
- Equipamentos sem supervisão.

9. CONTROLO DE ACESSOS

Todos os sistemas de informação do Grupo Amper devem ter um sistema de controlo de acesso. O controle de acesso também se concentra em garantir o acesso dos usuários e impedir o acesso não autorizado a sistemas de informação, incluindo medidas como a proteção por senha. O controle de acesso deve ser entendido tanto de um ponto lógico (centrado em sistemas de informação) como de um aspecto físico (ver secção 11 Segurança física e ambiental).

9.1 REQUISITOS EMPRESARIAIS PARA O CONTROLO DE ACESSO

O Grupo Amper assumirá uma série de requisitos empresariais para o controle de acesso, que serão pelo menos os seguintes: Os usuários serão únicos e não poderão ser compartilhados. Da mesma forma, os privilégios dos usuários serão inicialmente atribuídos pelo princípio de privilégio mínimo. Sempre que possível, deve ser utilizado um fator de autenticação múltipla (MFA) para o acesso aos sistemas de informação, sendo obrigatório para aqueles acessíveis a partir de redes públicas.

9.2 DIREITOS DE ACESSO

O Grupo Amper deve implementar controles de acesso que garantam que os usuários só recebam os privilégios e direitos necessários para desempenhar sua função. Os direitos de acesso devem ser estabelecidos com base em:

- Controle de acesso baseado em papéis: os perfis ou papéis de acesso devem ser definidos pelo aplicativo e/ou sistemas para atribuí-los a diferentes usuários.
- Necessidade de saber: o acesso a um recurso só será permitido quando houver uma necessidade legítima para o desenvolvimento da atividade.
- Privilégios mínimos: as permissões concedidas aos usuários devem ser o mínimo.
- Segregação de funções: deve assegurar-se uma segregação adequada de funções para desenvolver e atribuir direitos de acesso.

Nenhum utilizador pode aceder unicamente a um sistema de informação controlado sem a aprovação do utilizador responsável (ou da pessoa designada).

9.3 CONTROLO DE ACESSO LGICO

O Grupo Amper deve estabelecer uma política de senhas adequada alinhada com boas práticas de segurança. A política de senhas definirá os requisitos de senha e os tempos de manutenção para a mesma senha. A Política de Senhas deve ser conhecida por todos os funcionários do Grupo Amper.

9.4 TELETRABALHO

O acesso remoto à rede das empresas do Grupo Amper deve ser controlado sob a forma de trabalho à distância, ou seja, de fora das próprias instalações. Os serviços de ligação laboral remota serão destinados exclusivamente ao pessoal do Grupo Amper. Seu uso por qualquer outro parceiro exigirá autorização do agente de segurança. O equipamento utilizado para a conexão em modo de trabalho remoto pode ser propriedade do empregado ou fornecido pelo Grupo Amper. Em qualquer caso, é obrigatório que o computador atenda aos seguintes requisitos de segurança: a) Capacidade de estabelecer uma conexão através de uma VPN. b) Ter um sistema operacional atualizado com os últimos patches e atualizações de segurança. c) Instalação de software antivírus. d) Software de firewall/firewall pessoal instalado. O teletrabalho a partir da própria equipe de um trabalhador exigirá todas as medidas de segurança adequadas, com o objetivo de garantir que o trabalho remoto não represente uma ameaça para a segurança das informações do Grupo Amper. Além disso, medidas de segurança adicionais podem ser implementadas para garantir uma conexão remota mais confiável e segura. O serviço de teletrabalho será monitorado e monitorado, registrando tanto a conexão quanto a atividade de acordo com os protocolos de segurança.

10 IDENTIDADE DE GESTO DO CICLO DE VIDA

As empresas do Grupo Amper definirão e implementarão um sistema adequado para gerir o ciclo de vida da identidade. A identidade é o conjunto de características que identificam de forma única qualquer pessoa com acesso físico ou lógico aos sistemas de informação do Grupo Amper. O ciclo de vida da identidade é o processo que segue a identidade de um usuário desde sua criação até sua eliminação. O ciclo de vida da identidade consiste nas seguintes atividades:

a) Criação e atribuição de identidade

b) Revisão periódica

c) Modificação ou eliminação

A gestão deste ciclo requer definir os requisitos de segurança e responsabilidades de cada etapa, a fim de centralizar e facilitar os processos de gestão associados a elas. A gestão do ciclo de vida da identidade deve estar alinhada com o Departamento de Recursos Humanos com o objetivo de verificar as identidades com base nas demissões e baixas dos funcionários e sua correspondência nos sistemas de informação.

10.1 IDENTIDADES PRIVILEGIADAS

A atribuição e uso dos direitos de acesso privilegiados deve ser restrita e controlada. O acesso privilegiado é o acesso a sistemas como administrador ou com uma função que oferece a possibilidade de modificar a configuração do sistema. A atribuição de direitos de acesso privilegiado deve ser supervisionada através de um processo formal de autorização de acordo com as políticas de controle de acesso. Pelo menos os seguintes requisitos devem ser considerados:

- Devem ser identificados os direitos de acesso privilegiados associados a cada sistema ou processo (por exemplo, sistema operacional, sistema de gerenciamento de banco de dados ou aplicativo) e os usuários a quem devem ser atribuídos.
- A atribuição de direitos de acesso privilegiado deve ser baseada nas necessidades de uso, com base no privilégio mínimo e na necessidade de saber.
- Deve ser definido um processo de autorização que inclua o registro de privilégios. Os direitos de acesso privilegiado não devem ser concedidos até que o processo de autorização seja concluído.
- Devem ser definidos os requisitos para a expiração dos direitos de acesso privilegiado. As competências dos utilizadores com direitos de acesso privilegiado devem ser revistas periodicamente para verificar que cumprem as suas obrigações.

Devem ser estabelecidos e mantidos procedimentos e mecanismos específicos para evitar o uso não autorizado de contas genéricas de usuário para sua administração, de acordo com as capacidades de configuração do sistema. Devem ser estabelecidos procedimentos e mecanismos para garantir a confidencialidade das informações secretas de autenticação para usuários genéricos de gerenciamento (por exemplo, modificação frequente de senhas, mecanismos seguros de compartilhamento de senhas, etc.).

11 SEGURANA FSICA E AMBIENTAL

Os espaços físicos onde se encontram os sistemas de informação do Grupo Amper devem estar adequadamente protegidos mediante controlos de acesso perimetral, sistemas de vigilância e medidas preventivas para que o impacto de incidentes de segurança (acesso não autorizado a sistemas de informação, roubo ou sabotagem) e acidentes ambientais (incendios, inundações, cortes de luz, etc.) possa ser prevenido.

12. SEGURANÇA NO TRABALHO EM NUVEM

O Grupo Amper deverá manter uma política de trabalho em nuvem que estabeleça as medidas de segurança adequadas para garantir a **confidencialidade, integridade e disponibilidade da informação**. Dependendo do tipo de modelo de serviço em nuvem, deverão ser aplicadas diferentes medidas de segurança:

- **Infraestrutura (IaaS)**: em primeiro lugar, deverá ser assegurado que o Fornecedor monitoriza o ambiente para detetar alterações não autorizadas. Além disso, deverão ser estabelecidos níveis robustos de autenticação e controlo de acessos para os administradores e para as operações por eles realizadas. Por último, as instalações e/ou configurações dos elementos comuns deverão ser registadas e interligadas, de forma a garantir a rastreabilidade adequada.

- **Plataforma (PaaS)**: adicionalmente às medidas indicadas para o modelo de serviço de Infraestrutura, o Fornecedor do serviço deverá disponibilizar mecanismos de segurança correspondentes ao ciclo de vida de desenvolvimento seguro de software,

de acordo com a secção **15 – Segurança no Ciclo de Vida do Desenvolvimento de Sistemas**.

- **Software (SaaS)**: adicionalmente às medidas indicadas para o modelo de serviço de Plataforma, o Grupo Amper e o Fornecedor deverão seguir as orientações da **OWASP (Open Web Application Security Project)** como referência para a segurança das aplicações.

13 SEGURANA OPERATIVA

Todos os sistemas de informação da Amper Group que processem ou armazenem informações na sua propriedade devem contar com as medidas de segurança adequadas que otimizem o seu nível de maturidade adequado (monitoramento, controlo de alterações, revisões, etc.). As redes também devem ser gerenciadas, monitoradas e monitoradas adequadamente para proteger contra ameaças e manter a segurança dos sistemas e aplicativos que as utilizam, incluindo os controles de acesso à rede, protegendo as informações transferidas através desses elementos e/ou ambientes.

14 SEGURANA EM TELECOMUNICAES

A arquitetura de rede do Grupo Amper deve contar com medidas de prevenção, detecção e resposta para evitar lacunas nos domínios internos e externos. "Domínio interno" significa a rede local composta por elementos tecnológicos do Grupo Amper acessíveis exclusivamente a partir da rede interna. Por outro lado, "domínio externo" significa a rede acessível de fora da rede do Grupo Amper. A gestão da segurança das redes que atravessam o perímetro do Grupo Amper é de suma importância, já que introduz controles adicionais para os dados sensíveis que circulam através das redes públicas de comunicação. O Grupo Amper definirá as diretrizes de segurança a seguir na transferência de informações, as medidas de segurança no uso de equipamentos portáteis, serviços de Internet e e-mail, e controles específicos para conectar os sistemas de informação do Grupo Amper a partir de fora de suas instalações.

15 SEGURANA DO CICLO DE VIDA DO DESENVOLVIMENTO DE SISTEMAS

Todas as aquisições, desenvolvimento e manutenção de sistemas devem cumprir os requisitos mínimos de segurança necessários para o desenvolvimento de software, sistemas e dados, de acordo com as boas práticas do setor. Além disso, o gerenciamento de testes, o acompanhamento de alterações e o inventário de software devem ser realizados. Cada empresa do Grupo Amper deve levar em conta a segurança da informação em seus sistemas e processos de dados, procedimentos de seleção, desenvolvimento e implementação de aplicativos, produtos e serviços.

16. SEGURANÇA DOS FORNECEDORES

Deverá ser avaliada a criticidade dos serviços passíveis de subcontratação, com vista à identificação daqueles que sejam relevantes sob a perspetiva da segurança da informação, seja em razão da sua natureza, da sensibilidade dos dados a tratar ou da dependência relativamente à continuidade do negócio.

Relativamente aos fornecedores destes serviços, deverão ser assegurados procedimentos adequados de seleção, requisitos contratuais, incluindo disposições relativas à cessação contratual, monitorização dos níveis de serviço, devolução de dados e verificação das medidas de segurança implementadas pelo referido fornecedor, as quais deverão ser, no mínimo, equivalentes às estabelecidas na presente Política.

17. GESTÃO DE INCIDENTES

Todos os colaboradores do Grupo Amper têm o dever e a responsabilidade de identificar e comunicar ao responsável pela segurança da respetiva sociedade qualquer incidente ou infração suscetível de comprometer a segurança dos seus ativos de informação. Do mesmo modo, o Grupo Amper deverá implementar procedimentos adequados para a correta gestão dos incidentes detetados.

Deverá ser definido um procedimento de resposta a incidentes, no qual se estabeleça um processo de categorização dos incidentes, análise dos impactos no negócio e escalonamento, pela função de Segurança da Informação e Cibersegurança, de qualquer incidente relacionado com a segurança da informação.

18. CONTINUIDADE DO NEGÓCIO

Em conformidade com os requisitos de qualidade e as melhores práticas aplicáveis, o Grupo Amper deverá dispor de um Plano de Continuidade do Negócio, integrado na sua estratégia para garantir a continuidade da prestação dos seus serviços essenciais ou críticos e a adequada gestão dos impactos no negócio em eventuais cenários de crise, proporcionando um quadro de referência que oriente a atuação da sociedade sempre que necessário.

O referido Plano de Continuidade deverá ser revisto, atualizado e testado periodicamente. Adicionalmente, deverá ser definido e mantido atualizado um Plano de Recuperação de Desastres, alinhado com a estratégia de continuidade do negócio, o qual abrangerá a continuidade do funcionamento das tecnologias de informação e comunicação.

O Grupo Amper deverá assegurar a formação e capacitação de todos os seus colaboradores em matéria de Continuidade do Negócio. A formação nesta matéria deverá ser objeto de

revisão periódica, com o objetivo de garantir o seu pleno alinhamento com o Plano de Continuidade do Negócio em vigor.

19. AUDITORIAS DE SEGURANÇA E GESTÃO DE VULNERABILIDADES

Deverão ser identificadas periodicamente as vulnerabilidades técnicas dos sistemas de informação e das aplicações utilizadas pela organização, em função do respetivo grau de exposição a tais vulnerabilidades, devendo ser adotadas medidas adequadas para mitigar os riscos associados.

Uma vez identificadas as vulnerabilidades, a organização deverá implementar as medidas corretivas necessárias com a maior brevidade possível. A identificação, gestão e correção das vulnerabilidades deverão ser realizadas de acordo com uma abordagem baseada no risco, tendo em consideração a criticidade dos ativos e o respetivo nível de exposição.

20 ANEXOS

20.1 ANEXO: NVEIS DE CLASSIFICAO

Nível	Nível de detalhe	Exemplos
Uso público	Esta é informação que pode ser conhecida por qualquer tipo de pessoa e seu uso fraudulento não representa um risco para os interesses do Grupo Amper	Exemplos deste tipo de informação são catálogos de produtos e as informações disponíveis no site.
Difusão limitada	é a informação utilizada pelas áreas do Grupo Amper e cujo uso fraudulento supõe um risco para os interesses do Grupo que não é significativo	Os e-mails e documentos de trabalho das áreas do Grupo são exemplos desse tipo de informação.
Informações confidenciais	confidenciais são informações que só um pequeno número de pessoas pode conhecer e para as quais o uso fraudulento pode ter um impacto significativo nos interesses do Grupo Amper.	Exemplos deste tipo de informação são os relatórios de auditoria e estratégia do Painel.
Informação reservada	é a informação que só deve ser conhecida pelo proprietário do mesmo e cuja divulgação pode causar danos graves aos interesses do Grupo.	Exemplos são a comunicação entre altos executivos ou acionistas com decisões relevantes para a operação empresarial.
A informação secreta	é aquela cuja divulgação não autorizada pode causar um	. Exemplos são chaves criptográficas, informações

	danos excepcionalmente graves aos interesses essenciais do Grupo.	de fusões ou aquisições, ou qualquer outra informação que possa colocar em risco o valor da ação.