Ordem de Serviço
n.º BAE 002/22

Origem:		Classificação:	Interno (I)
BAE		Emissão:	17.01.2022
Comissão Executiva		Entrada em vigor:	17.01.2022
Destinatários:		Expira:	
Grupo Brisa		Revoga:	OS nº BAE 004/20
Assunto:	Normas de Funcionamento		
Sub-Assunto:	Política e Normas de Segurança da Informação do Grupo Brisa		

SÍNTESE

Atualiza a política e normas que estão subjacentes à segurança da informação do Grupo Brisa, incluindo a sua classificação, processamento e as responsabilidades dos diversos intervenientes na sua utilização.

ÍNDICE

50 ANOS A TRANSFORMAR PORTUGAL

1. INTRODUÇÃO

Entende-se como informação, um conjunto de dados obtidos de forma precisa e temporalmente enquadrada que, depois de organizados com um determinado objetivo e apresentados dentro de um contexto que lhes confira significado e relevância, contribuem para o aumento da compreensão ou diminuição da incerteza relativamente a um determinado tema ou assunto.

A informação pode existir em diversos formatos: impressa ou escrita em papel, armazenada fisicamente ou eletronicamente, transmitida pelo correio ou através de meios eletrónicos, disponibilizada em suporte de vídeo e/ou áudio ou transmitida verbalmente.

No desenvolvimento dos negócios do Grupo Brisa, a informação é um ativo essencial uma vez que leva ao aumento do conhecimento e diminuição da incerteza, afetando os comportamentos, as tomadas de decisão e, consequentemente, os resultados finais. Torna-se, assim, necessário criar mecanismos para a sua salvaguarda e proteção, tendo em conta o seu valor.

O presente documento tem como objetivo definir a política e as normas de segurança da informação do grupo, a cumprir por todos os colaboradores dos órgãos/empresas, bem como pelas entidades externas sob a sua responsabilidade.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A política de segurança da informação contém as normas que visam garantir a preservação de toda a informação referente às empresas do Grupo Brisa, sob sua guarda ou que lhes tenha sido, por qualquer modo, transmitida ou seja por estas registada, visando e/ou tendo subjacente:

- Vincular os órgãos/empresas e os respetivos colaboradores à necessidade de assegurarem a confidencialidade, a integridade e a disponibilidade da informação;
- Salvaguardar a proteção de dados pessoais dos colaboradores, de clientes, de fornecedores e de parceiros e de quaisquer outras pessoas ou entidades;
- Estabelecer mecanismos de controlo e de proteção da informação, de forma a prevenir e mitigar o risco de destruição, uso inadequado, furto, acesso, cópia, alteração ou divulgação não autorizados ou indevidos;
- Assegurar que as entidades externas que prestem serviços ou qualquer tipo de colaboração aos órgãos/empresas do grupo, cumprem os requisitos definidos no presente documento;
- Garantir o acesso à informação e a sua utilização em conformidade com a regulamentação e legislação em vigor, bem como, com as políticas do grupo.

Esta política aplica-se a todo o tipo de informação criada ou utilizada como suporte à atividade dos órgãos/empresas, que se encontre registada em algum tipo de suporte físico, eletrónico ou outro, independentemente do seu formato, tecnologias que a suportem, ou tipo e condições de armazenamento.

Compete a todos os colaboradores do grupo, bem como a terceiros, salvaguardar os interesses da organização, contribuindo proactivamente para a proteção da informação, através do cumprimento da presente política, normativos internos e legislação em vigor. Em caso de incumprimento estes poderão ser disciplinarmente ou judicialmente responsabilizados.

3. CONCEITOS BASE DE SEGURANÇA DE INFORMAÇÃO E SUA APLICABILIDADE

A segurança da informação consubstancia-se nos seguintes conceitos base:

- Confidencialidade: garante que o acesso a determinada informação se restringe a quem está devidamente credenciado e autorizado para tal;
- Integridade: garante que a informação processada é fidedigna, mantendo todas as características originais estabelecidas;
- Disponibilidade: garante que a informação está sempre disponível para uso legítimo, ou seja, por todos aqueles que estão autorizados a utilizá-la, sempre que necessário.

Para a gestão da informação ser eficaz, é fundamental que o nível de sensibilidade da informação seja especificado pelos órgãos/empresas, tendo por base critérios de confidencialidade, integridade e disponibilidade.

3.1. Confidencialidade

A confidencialidade de um determinado conjunto de informação é determinada pelos órgãos/empresas de acordo com os seguintes níveis e critérios:

Informação	Descrição
Público (P)	Informação que pode ser livremente partilhada com qualquer pessoa interna ou externa, por essa partilha não comprometer os objetivos e/ou a imagem do grupo.
Interno (I)	Informação relevante para o desenvolvimento da atividade do grupo cuja divulgação ao exterior fica sujeita a prévia validação, para que o acesso por parte de entidades externas não comprometa os objetivos, a proteção do *know-how* e/ou a imagem do grupo. Esta informação deve ser partilhada, apenas, com os colaboradores do grupo ou com órgãos/unidades de negócio específicas. A disponibilização deste tipo de informação a pessoas externas ao grupo, mesmo ao abrigo de algum tipo de prestação de serviços ou colaboração, carece de autorização prévia por parte do órgão/empresa responsável pela informação e devem ser assegurados os termos da sua utilização pela entidade que a receba designadamente que não faz dela utilização pública não autorizada.
Interno com dados Pessoais (IP)	Informação interna que contém dados pessoais relevante para o desenvolvimento da atividade do grupo, mantendo-se o referido no ponto anterior, no âmbito da informação "Interno (I)".
Confidencial (X)	Informação determinante para o sucesso dos negócios do grupo, ou que seja classificada legalmente ou contratualmente como tal. Esta informação é restrita a um conjunto específico de pessoas (colaboradores e/ou parceiros), explicitamente indicadas pelo nome, sendo o seu acesso devidamente autorizado pelo respetivo responsável do órgão/empresa, tendo por base o estritamente necessário para o desempenho de uma determinada função ou atividade ou o estabelecido na lei sobre a respetiva proteção, por a sua divulgação poder causar danos com impacto muito elevado no negócio, na imagem, comprometer a missão e estratégia do grupo e/ou violar obrigações legais ou contratuais. O acesso por entidades externas a dados pessoais está sujeito a prévia autorização do responsável do órgão/empresa, por meio passível de ser comprovado sempre que necessário limitado ao estritamente necessário ao exercício da atividade contratada ou ao estabelecido na lei.
Reservado (S)	Informação com classificação de segurança de âmbito restrito aos Quadros Dirigentes do grupo.

A classificação da informação pode ser dinâmica, sendo que, informações classificadas em determinado momento como confidenciais, podem ser públicas, num outro momento. Adicionalmente, note-se que a classificação da informação não prejudica os deveres aos quais as várias entidades do grupo estão sujeitas ao abrigo de legislação que regule a respetiva informação, nomeadamente a de tratamento de dados pessoais.

3.2. Integridade

Deve ser garantida a integridade de toda a informação armazenada, de forma a assegurar que todas as informações são preservadas de forma autêntica, i.e., no seu formato original, exato e completo, sem quaisquer alterações, com vista a que estas sirvam os propósitos para os quais foram designadas.

A garantia da integridade da informação tem como base a definição clara, na organização, dos colaboradores responsáveis pela sua manipulação, materializado através da definição de controlos do acesso à mesma, sendo essencial a definição de orientações e identificação dos respetivos riscos para a subsequente implementação de controlos e mecanismos de segurança (*firewall*, definição e revisão de perfis de acesso, criptografia, *backups*, entre outros) mediante a sua criticidade para os órgãos/empresas.

3.3. Disponibilidade

A disponibilidade a informação deve ser classificada, pelos órgãos/empresas, em função do risco que a perda das suas características e/ou a sua indisponibilidade acarretam para a atividade da empresa, considerando-se, para o efeito, os seguintes níveis:

Informação	**Descrição**
Muito crítica	Quando o processamento não autorizado da informação, perda ou destruição por meio de atividade maliciosa, acidente ou gestão irresponsável, cause perdas de difícil recuperação ou mesmo irrecuperáveis, com custos financeiros muito significativos, colocando o órgão/empresa numa situação de incumprimento legal e/ou contratual e com impacto reputacional adverso junto das partes interessadas
Crítica	Quando o processamento não autorizado da informação, perda ou destruição por meio de atividade maliciosa, acidente ou gestão irresponsável, cause perdas ou danos que, ainda que recuperáveis, têm custos financeiros significativos, colocando o órgão/empresa numa situação de incumprimento legal e/ou contratual e com impacto reputacional adverso junto das partes interessadas
Não crítica	Quando o processamento não autorizado da informação, perda ou destruição, cause pouco mais do que um transtorno temporário, com custos de recuperação limitados e sem qualquer impacto adverso junto das partes interessadas

De forma a proteger a informação Muito Crítica ou Crítica, deve-se verificar, periodicamente, a respetiva integridade, o cumprimento do regime de acessos, bem como, sendo o caso, garantir que existe um segundo repositório, em local distinto, que permita a recuperação da informação em caso de desastre/catástrofe.

As medidas para proteger informação considerada Não Crítica, incluem o armazenamento de cópias em locais fechados e mecanismos de controlo de acessos, que impeçam que pessoas não autorizadas possam aceder e processar a informação existente.

4. SALVAGUARDA, TRATAMENTO E PROTEÇÃO DA INFORMAÇÃO

4.1. Formalização de Obrigações de Confidencialidade e Sobre o Tratamento da Informação

No âmbito da contratação de serviços a entidades externas, o acesso por estas à informação deve ser sempre avaliado e, se necessário ou conveniente, analisadas alternativas.

Caso se verifique que o acesso é realmente necessário, os órgãos/empresas responsáveis pelo acompanhamento destas entidades, devem efetuar as diligências necessárias no sentido de garantir o compromisso de confidencialidade e de tratamento de informação entre as partes, com vista a salvaguardar os interesses do grupo e o cumprimento de obrigações legais ou contratuais de confidencialidade.

Aquando da formalização de uma relação contratual com um terceiro, além do cumprimento da legislação e das normas em vigor e das políticas internas aplicáveis – nomeadamente a Política de Gestão de Compras do Grupo Brisa – deve ser garantida, em estreita colaboração com a Direção Jurídica (DJR) da Brisa Auto-Estradas (BAE), a existência de acordos (obrigações) de confidencialidade e de tratamento da informação, sempre que a entidade externa:

- Aceda a informações dos órgãos/empresas e/ou compartilhe informações sobre a sua atividade;
- Aceda e/ou partilhe informações associadas a propostas comerciais ou quaisquer outras informações que se encontram legal ou contratualmente sujeitas a obrigações de confidencialidade;
- Aceda e/ou partilhe dados pessoais (colaboradores, clientes, entre outros).

Adicionalmente, os colaboradores devem, quando acederem a informação de uma entidade externa atuar nos termos do acordo de confidencialidade e/ou cláusula específica em vigor entre as partes.

No caso de não existir acordo de confidencialidade e de tratamento da informação, ou qualquer norma específica sobre o assunto, os colaboradores devem, quanto à informação confidencial de uma entidade externa confiada ao seu cuidado, tratá-la de acordo com o aqui disposto relativamente à informação confidencial do grupo, sem prejuízo dos princípios e normas aplicáveis por via de outras políticas e procedimentos do grupo.

Os colaboradores devem imediatamente informar o seu superior hierárquico assim que tomarem conhecimento da divulgação ou posse não autorizada de informação confidencial por terceiros, bem como adotar as medidas razoáveis para minimizar ou corrigir a disseminação e/ou divulgação da informação em causa.

Nos casos de projetos pontuais em que os colaboradores envolvidos tenham a necessidade de aceder a informação confidencial de particular sensibilidade, interna ou de terceiros, aos colaboradores envolvidos pode ser solicitada a assinatura de um documento, evidenciando que tomaram conhecimento das características da informação tratada e do nível de confidencialidade exigido. Este documento visa reforçar as obrigações constantes nesta política e deixar claro o caráter de confidencialidade e sensibilidade da informação em causa.

4.2. Tratamento da Informação Confidencial

Os colaboradores e entidades externas contratadas que tenham acesso a informação confidencial devem ser claramente identificados, quer através do nome quer pelas funções que exercem, ou no caso das entidades externas, pelo nome da empresa e ou do da pessoa individual e pelas atividades que executem.

O acesso à informação confidencial só pode ser concedido após permissão dos respetivos responsáveis dos órgãos/empresas, devendo esta autorização ser documentada física ou eletronicamente.

Para a informação classificada como confidencial, deve ser garantido pelos responsáveis dos órgãos/empresas que:

- Os registos tangíveis (documentos em papel, entre outros) são:
  - Armazenados em locais de acesso restrito, quando não estiverem a ser utilizados, sendo o acesso a estes locais limitado a pessoas autorizadas;
  - Fisicamente destruídos, quando deixarem de ser necessários, ou, no caso de dados pessoais, quando esgotado o prazo de conservação definido;
- Qualquer informação que seja transmitida deverá ser, sempre que possível, encriptada, exceto nos casos em que tal seja proibido por lei;
- Os equipamentos portáteis e/ou outros dispositivos de armazenamento móveis e/ou externos que tenham este tipo de informação armazenada, dispõem de tecnologia de encriptação;
- Os servidores que armazenam informação confidencial devem ser protegidos por barreiras de segurança perimétricas, permitindo apenas conexões com sistemas autorizados, utilizando para o efeito, exclusivamente, protocolos aprovados.

5. DISPOSIÇÕES FINAIS

Todas as situações omissas na presente Ordem de Serviço, ou que suscitem dúvidas, devem ser encaminhadas à Direção de Auditoria, Organização e Qualidade (DAQ) da BAE, a quem cabe a procura da solução mais adequada e/ou esclarecimento.

É da responsabilidade da Comissão Executiva (CE) da BAE, a aprovação desta política, a qual será objeto de revisão periódica, sempre que necessário, por forma a manter o máximo rigor e excelência no que se refere aos princípios e linhas de orientação adotados.

São Domingos de Rana, 17 de janeiro de 2022

António Pires de Lima, *Presidente da Comissão Executiva*