POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NA RELAÇÃO COM FORNECEDORES

▪ Conhecimento da Política

Esta Política deve ser disponibilizada a todos os fornecedores com acesso a ativos de informação e/ou às instalações da DUO Capital, durante a relação contratual, como adenda ao contrato de prestação de serviços ou, nos casos já anteriormente contratualizados, através do envio de uma circular, e-mail ou outra forma documentada.

▪ Acordo documentado

Deve ser estabelecido em contrato, ou pelo menos em acordo documentado, com os Fornecedores não certificados na ISO/IEC 27001 quais as regras de segurança da informação a cumprir, nomeadamente:

- Níveis de serviço (SLA – Service Level Agreement) assumidos;
- Formação e sensibilização dos seus colaboradores, de forma a garantir uma prática em conformidade com as regras legais de segurança da informação e proteção de dados pessoais;
- Comunicação aos seus colaboradores dos requisitos acordados no contrato, de forma a assegurar o seu cumprimento;
- Reporte de incidentes de segurança da informação de imediato, sempre que ocorram.

▪ Declaração de Confidencialidade ou de Não Divulgação

Os fornecedores envolvidos num processo de aquisição de produtos e/ou serviços, no qual aqueles necessitem de ter acesso a informação sensível, devem assinar uma **Declaração de Confidencialidade ou de Não Divulgação**, que poderá ou não estar incluída no próprio contrato de aquisição de produtos e/ou serviços.

Os acordos de confidencialidade ou não divulgação devem ser elaborados de forma a proteger informação confidencial, respeitando a legislação aplicável.

Estes acordos devem considerar os seguintes pontos:

- Definição da informação a ser protegida (informação confidencial e dados pessoais);
- Duração expectável do acordo, incluindo prazos para a manutenção da confidencialidade;
- Ações necessárias quando o acordo termina, incluindo condições para a devolução ou destruição de informação;
- Responsabilidades para evitar divulgação de informação não autorizada;
- Propriedade da informação, propriedade intelectual e proteção de informação comercial;
- O uso permitido de informação confidencial e os direitos de autor para usar a informação;
- O direito de auditar as atividades que envolvam informação confidencial;
- Processo para notificar e reportar divulgação não autorizada ou fuga de informação confidencial;

- Ações em caso de quebra de acordo.

Requisitos de Segurança da Informação por Fornecedor

Sempre que se verifique a necessidade de existência de contrato ou equiparável, estes incluirão a obrigação de cumprimento de requisitos de confidencialidade da informação e proteção de dados pessoais, conforme pontos anteriores e respeitando, pelo menos, o seguinte:

Tipos de Fornecedor	Requisitos de segurança da informação	Ativos de informação acedidos	Classificação da informação
Serviços de Comunicações	SLA (níveis de serviço) Taxa disponibilidade	Rede/internet	Confidencial
Serviços de manutenção TI	SLA (níveis de serviço) Contrato c/ acordo de confidencialidade	Hardware	Confidencial
Serviços de suporte (service desk)	SLA (Níveis de serviço) Contrato c/ acordo de confidencialidade	Software	Confidencial
Serviços Cloud	SLA (Níveis de serviço) Taxa disponibilidade Contrato como subcontratante Certificação ISO 27001	Software e ficheiros	Confidencial
Serviços de limpeza	Acordo de Confidencialidade Formação/sensibilização Lista de pessoas autorizadas a aceder à instalação	Instalações	Interno
Serviços de vending	Acordo de Confidencialidade	Instalações	Interna
Serviços consultoria	Contrato de prestação serviço Acordo de Confidencialidade	Documentos sensíveis da organização	Confidencial
Trabalho Temporário	Contrato de prestação serviço Acordo de confidencialidade	Documentos	Confidencial

Acesso às Instalações da DUO Capital

O acesso às instalações deve respeitar as seguintes regras:

- Os fornecedores que acedam às instalações devem estar sempre acompanhados;
- O acesso à rede *wireless* só é permitido para a rede de visitantes sendo fornecida a senha de acesso para a rede de visitantes;
- A utilização de discos portáteis ou PEN dentro das instalações, pelos prestadores de serviço, não é permitida a menos que explicitamente autorizado pelo *Management Team.*

Lista de Fornecedores

Os Fornecedores com acesso a ativos de informação e/ou às instalações da DUO Capital estão devidamente identificados na **Lista de Fornecedores**.

Incumprimento da Política

As não-conformidades ou violações às políticas ou procedimentos de segurança são passíveis de penalização e/ou quebra de contrato.