Medidas de Segurança Técnicas e Organizativas

Procedimentos de segurança da informação

Organização interna

Funções e responsabilidades separadas foram definidas para a segurança da informação e foram atribuídas aos responsáveis pela empresa pelas atividades de tratamento (doravante designados também por "usuários"), de forma a evitar conflitos de interesse e impedir atividades impróprias.

Segurança de recursos humanos

Dispositivos móveis e teletrabalho

Existe uma política de segurança para o uso de todos os dispositivos da empresa, em particular dispositivos móveis, e controles adequados estão em vigor.

Conclusão ou mudanças na relação de emprego

Após a cessação de uma relação de colaboração de um usuário na organização ou no caso de uma alteração significativa nas suas funções, as permissões de acesso são atualizadas imediatamente, enquanto as ferramentas de negócios são retornadas e redefinidas física e logicamente.

Gestão de recursos da empresa

Responsabilidade pelos recursos e ativos da empresa

Todas as ferramentas e ativos da empresa são cuidadosamente inventariados e a alocação dos mesmos aos vários usuários responsáveis pela sua segurança é fiscalizada. Foi definida uma política para o seu uso correto.

Classificação de informação

Todas as informações são classificadas e catalogadas pelos respetivos usuários, de acordo com os requisitos de segurança, bem como processadas adequadamente.

Gestão de storage media

As informações armazenadas em dispositivos de armazenamento (storage media) são geridas, controladas, modificadas e usadas de maneira a não comprometer seu conteúdo e são apagadas de maneira apropriada.

Controlo de acessos

Requisitos de controlo de acessos

Os requisitos organizativos da empresa para fiscalizar o acesso aos recursos de informação são documentados numa política e implementados na prática por meio de um procedimento de controlo de acessos; significando que o acesso à rede e conexões é limitado.

Gestão de acesso do usuário

A alocação de direitos de acesso dos usuários é controlada desde o registo inicial do usuário até a remoção dos direitos de acesso quando eles não sejam mais necessários, incluindo restrições especiais aos direitos de acesso privilegiado e a gestão de "informações secretas de autenticação", e está sujeita a revisões e verificações periódicas incluindo uma atualização dos direitos de acesso quando necessário. Na gestão de acesso, o critério de minimização de direitos de acesso é utilizado, pois são emitidos para conceder ao usuário apenas acesso aos dados necessários para a sua função e atividade comercial. Direitos de acesso adicionais requerem autorização específica.

Responsabilidade do usuário

Os usuários estão cientes das suas responsabilidades também por meio da manutenção da eficácia dos controlos de acesso, devendo, por exemplo, escolher palavras-passe complexas, cuja complexidade é verificada pelo sistema, e mantê-las confidenciais.

Sistemas e aplicações de controlo de acesso

O acesso às informações está sujeito a restrições em conformidade com a política de controlo de acesso, por meio de um sistema de acesso seguro e

gestão de palavras-passe, bem como controlos sobre usuários privilegiados e acesso limitado a todos os códigos-fonte.

Encriptação

Controlo criptográfico

Existe uma Política em vigor sobre o uso de criptografia de storage media e dados dos usuários. As autenticações são criptografadas.

Segurança física e ambiental

Estão em vigor medidas de segurança física e ambiental para impedir o acesso, a perda ou a disseminação ilegítima ou acidental de dados.

Áreas seguras: Data center

Os serviços da empresa são fornecidos e hospedados em vários Datacenters nacionais neutros, disponibilizados por fornecedores sob o formato de prestação de serviços. Todos os Datacenters, dentro da cadeia de fornecedores, oferecem redundância completa de todos os circuitos elétricos, de refrigeração e de rede. Todos os Datacenters têm iluminação de perímetro, bem como um sistema de deteção de presença com câmaras de CCTV, fornece a segurança privada do edifício, encontrando-se presente uma equipa de segurança 24/7 nos Datacenters.

O acesso físico é regulado e controlado por procedimentos de autorização, reconhecimento e registo e é limitado, graças ao sistema de controlo de acesso, às áreas para as quais existe uma autorização.

Equipamento

Existe uma política para abate de equipamentos sem utilização, a fim de destruir com segurança todas as informações que neles possam estar contidas.

Segurança das operações

Procedimentos e responsabilidades operacionais

As responsabilidades operacionais em TI são documentadas e as mudanças nas instalações e sistemas de TI são controladas. Sistemas de

desenvolvimento, sistemas de verificação e sistemas operacionais são separados.

Existem usuários responsáveis pelo bom funcionamento dos procedimentos. Por outro lado, a gestão da segurança lógica dos sistemas operacionais e das aplicações instaladas pelo cliente é de responsabilidade do cliente dos serviços individuais prestados pela Empresa (doravante também designado por "cliente").

Proteção contra malware

O controlo de vírus e malware está ativo nos dispositivos da empresa e existe uma consciencialização apropriada dos usuários.

No que diz respeito aos serviços do Servidor Virtual ou Servidor Dedicado, o cliente é responsável pela instalação de software antivírus e anti-malware e - se o serviço relacionado não tiver sido adquirido - de uma firewall. Com relação ao serviço de alojamento, existe uma proteção em tempo real nas máquinas de frontend.

No que diz respeito ao serviço de e-mail, o tráfego de e-mail é analisado em tempo real, tanto de entrada como de saída, para a deteção de vírus, malware e para a identificação e filtragem de spam. A análise é automatizada e baseia-se na natureza do conteúdo, na interrogação de bancos de dados internacionais e na reputação adquirida devido a uma série de parâmetros.

Cópia de segurança

São realizados backups periódicos, com a exclusão de serviços pelos quais o cliente não subscreveu serviço de backup e consequentemente é responsável por manter e gerir os seus backups. Para serviços de alojamento e

de correio, são realizados backups periódicos que, para serviços de alojamento, também podem ser acedidos pelo cliente. Backups adicionais, não acessíveis pelos clientes, são realizados com o único propósito de recuperação de desastres.

Autenticação e Monitoramento

Autenticação e Sincronização

Toda a atividade e eventos relacionados com a segurança das informações, realizados por usuários do sistema e administradores / operadores, ocorre após a inserção das suas credenciais de autenticação ou dos seus certificados de identidade. Os relógios de todos os equipamentos estão sincronizados.

Controlo de software operacional

A instalação de software nos sistemas operacionais é controlada e monitorizada.

Relativamente aos Servidores Virtuais e Servidores Dedicados, os sistemas operativos disponíveis para os clientes são disponibilizados com imagens de instalação atualizadas. Também é responsabilidade do cliente atualizar as aplicações ou software instalados pelo mesmo.

Segurança das comunicações

Gestão de segurança de rede

Redes e serviços online também são garantidos através da separação e segregação. A rede é monitorizada 24/7 quer ao nível das métricas assim como a alarmística automática.

Transferência de informação

Acordos relativos à transferência de informações de e para terceiros estão em vigor.

Aquisição, desenvolvimento e manutenção do sistema

Segurança em processos de desenvolvimento e suporte

As regras que governam a segurança do desenvolvimento de software e sistema são definidas numa Política. As alterações no sistema (para aplicativos e para sistemas operativos) são controladas. A segurança do sistema é testada e os critérios de elegibilidade, que incluem aspetos de segurança, são definidos.

Relacionamento com fornecedores

Segurança da informação no relacionamento com fornecedores

Existem contratos ou acordos que visam proteger e regular o processamento de informações da organização e dos clientes acessíveis a terceiros que operam na área de TI e a outros fornecedores subcontratados que fazem parte de toda a cadeia de fornecedores.

Gestão de serviços prestados por fornecedores

A prestação de serviços prestados pelos fornecedores é monitorizada e verificada em relação ao contrato ou acordo. As alterações no serviço são verificadas.

Gestão de incidentes para segurança das informações

Gestão de incidentes de segurança da informação e melhorias

Existem responsabilidades e procedimentos específicos que visam administrar coerentemente e efetivamente todos os eventos e incidentes relacionados à segurança da informação (por exemplo, o chamado procedimento

de violação de dados).

Aspetos de segurança da informação relacionados com a continuidade dos negócios

Redundâncias

Todas as principais instalações de TI são redundantes para atender aos requisitos de disponibilidade. Onde esta redundância não está em vigor, medidas adequadas estão em vigor para garantir a continuidade do serviço ou a minimização da perda de dados.

Conformidade

Cumprimento dos requisitos legais e contratuais

A empresa identifica e documenta as suas obrigações para com autoridades externas e outros terceiros em relação à segurança da informação, incluindo propriedade intelectual, documentação contábil e informações sobre privacidade.

Revisão da informação de segurança

Os projetos da organização relacionados à segurança da informação e às políticas de segurança são revistos e ações corretivas são tomadas quando necessário.