1. Finalidade

Assegurar que os controles sejam devidamente aplicados nos recursos de informação da Teleperformance Brasil, bem com o nível adequado de proteção, conforme os princípios fundamentais de segurança, são eles: confidencialidade, integridade e disponibilidade.

2. Introdução

Prover uma orientação clara a todos os, colaboradores, clientes, parceiros de negócio e terceiros quanto a segurança da informação de acordo com os requisitos, objetivos e estratégias de negócio utilizando as leis e regulamentações relevantes, com o propósito de estabelecer uma cultura de conscientização e comprometimento pela proteção dos ativos da Informação no que diz respeito a confidencialidade, integridade e disponibilidade, devidamente alinhado com apoiado pela a alta direção.

3. Abrangência

Esta política abrange todos os ativos de informação utilizados pela empresa, e os respectivos recursos que processam, armazenam e transmitem tais informações, para o desenvolvimento de seus negócios e é aplicada, com caráter obrigatório, a toda a organização, e consequentemente a toda e qualquer pessoa que possa ter acesso a informação.

4. Definições

Segurança da Informação: preservação da confidencialidade, da integridade e da disponibilidade da informação a fim de assegurar a continuidade do negócio, minimizar o risco do negócio e maximizar o retorno sobre investimentos e oportunidades de negócio.

Acesso: direito de utilizar sistemas de computação. Para ver, instruir, comunicar, armazenar dados, resgatar dados, ou outra forma de uso de computadores e recursos de informação.

Ativos e/ou Recursos de Informação: tudo que tem valor para a empresa (procedimentos, equipamentos, localizações, *software* e dados que são desenhados, construídos, operados e mantidos para coleta, registro, processar, armazenar, resgatar, visualizar e transmitir informações.

Proprietários de Informação: é o funcionário com cargo de gerência que decide sobre a finalidade, conteúdo e uso do ativo de informação. Responsabiliza-se pelo cumprimento dos controles de segurança aplicáveis ao ativo, inclusive a classificação e severidade. Em alguns casos essa atribuição pode ser delegada a funcionários subalternos, contudo a responsabilidade pela informação é ainda do diretor ou gerente.

Usuário de Informação: indivíduos que usam ou tem acesso a recursos de informação da empresa, incluindo colaboradores, fornecedores e visitantes.

5. Política

A Segurança da Informação da Teleperformance Brasil deve ser mantida continuamente através do cumprimento pleno das Políticas, assim como do Manual de Segurança da Informação (MA-0003), dos Procedimentos e Instruções de Trabalhos derivados desta.

O Manual de Segurança da Informação (MA-0003) mantém um Sistema de Gestão de Segurança da Informação (SGSI) alinhado com os objetivos dos negócios e devidamente aprovado e apoiado pela alta direção.

O documento da Política de Segurança da Informação deve estar disponível e deve ser divulgado a todos os colaboradores e a qualquer pessoa que possa ter acesso a informações geradas em função dos negócios da empresa.

O uso dos recursos e/ou ativos de informação da Teleperformance Brasil devem ser somente para fins profissionais, de acordo com suas funções e atribuições de trabalho e responsabilidades, e não deve ser utilizado para benefício próprio ou para propósitos não relacionados ao negócio.

A Política de Segurança da Informação deve ser revisada anualmente ou sempre que mudanças significativas ocorrerem para garantir sua continuidade, adequação e efetividade.

5.1. Gerenciamento de Ativos

As diretrizes para o uso aceitável dos ativos de informação devem estar claramente identificadas e implementadas, conforme Política de Uso Aceitável de Recursos e Informação (PL-0026).

Além disso, devem ser adotadas diretrizes de mesa limpa para papéis e dispositivos removíveis, e uma política de tela limpa para recursos de processamento da informação, a fim de garantir que informações sensíveis não sejam expostas quando não estiverem sendo monitoradas pelo usuário, conforme Política de *Clear Desk* - Mesa Limpa (PL-0081).

As informações da Teleperformance Brasil devem estar classificadas quanto ao valor, requisitos legais, sensibilidade e criticidade. A classificação e os controles associados para a proteção das informações devem atender às necessidades do negócio da empresa quanto ao compartilhamento ou à restrição das informações e os impactos no negócio, associados a estas necessidades, estas descritas na Política de Classificação e Gestão da Informação (PL-0036).

A empresa concede aos colaboradores o privilégio de usar *smartphones* e/ou *tablets* pessoal no ambiente corporativo, desde que tenha necessidade e seja utilizado para fins profissionais, bem como as diretrizes do documento Política de Uso de Dispositivos Pessoais (BYOD) (PL-0077) sejam implementadas.

5.2. Segurança de Recursos Humanos

Todos os colaboradores devem concordar e assinar os termos e condições presentes em seus respectivos contratos de trabalho, aceitando suas responsabilidades em relação à Segurança da Informação.

Devem ser realizados treinamentos e programas de conscientização sobre Segurança da Informação periodicamente a todos os colaboradores da empresa.

Os direitos de acesso à informação de todos os colaboradores devem ser revogados em caso de desligamento, término de contrato, afastamento e férias ou devem ser devidamente ajustados em caso de mudança de atribuição.

Todos os colaboradores devem devolver à empresa todos os ativos que estejam em seu poder em caso de desligamento ou término de contrato, conforme Procedimento de Rescisão do Contrato de Trabalho (PQ-0037).

5.3. Segurança Física e do Ambiente

Os perímetros de segurança física devem estar claramente definidos e adequadamente protegidos para garantir a proteção das áreas que contêm ativos de informação.

Devem ser implementados controles apropriados de acesso físico que garantam que somente pessoas autorizadas tenham acesso às instalações e aos recursos da empresa.

Os usuários que não tiverem necessidade de negócio para acessar as instalações e recursos da empresa devem ter seus acessos revogados.

Todos os usuários devem possuir um crachá de identificação e devem utilizá-lo de forma visível.

Devem ser implementados controles e recursos que garantam a proteção física dos ativos da empresa contra danos provenientes de incêndio, enchente, explosão e quaisquer outras formas de desastres naturais ou causados pelo homem. Além disso, para a adequada proteção do ambiente físico devem ser seguidas as diretrizes do documento Política de Segurança Física (PL-0043).

5.4. Gerenciamento das Comunicações e Operações

Os procedimentos operacionais devem estar documentados, atualizados e disponíveis a todos que necessitarem ter acesso aos mesmos.

Além disso, as mudanças em recursos de processamento de informação devem ser controladas, conforme definidas as diretrizes na Política de Gestão de Mudanças (PL-0056).

Devem ser implementados controles para detecção, prevenção e recuperação, bem como medidas para conscientização dos usuários, a fim de proteger as informações de códigos maliciosos.

As redes devem ser adequadamente administradas e controladas, a fim de estarem protegidas de ataques e para manterem a segurança dos sistemas e aplicações que utilizam destes recursos, inclusive informações em trânsito.

As diretrizes e os controles formais para transmissão de informações devem estar implementados, a fim de proteger a troca de informações através do uso de todos os tipos de recursos de comunicação.

As informações em mensagens eletrônicas devem estar devidamente protegidas.

Os registros de auditoria sobre atividades dos usuários, exceções e eventos de Segurança da Informação devem ser produzidos e armazenados pelo período adequado ao tipo de informação, a fim de auxiliar em futuras investigações e monitoramento de controle de acesso.

Os horários de todos os sistemas que processam informações devem estar em perfeita sincronia com a fonte de horário padrão definida.

Adicionalmente, os controles e/ou diretrizes necessários para o adequado gerenciamento da segurança operacional e das comunicações estão definidos no documento Política de Segurança Operacional e nas Comunicações (PL-0068).

5.5. Controle de Acesso Lógico

As diretrizes de controle de acesso devem ser claramente estabelecidas, formalmente documentadas e revisadas, devendo estar baseadas nos requisitos de negócio e de Segurança da Informação, conforme documento Política de Gestão de Acessos Lógicos (PL-0066).

Os usuários devem ser conscientizados a seguir as boas práticas de Segurança da Informação ao selecionar e utilizar senhas.

Os usuários devem assegurar que seus equipamentos estejam protegidos adequadamente quando não estiverem sendo utilizados.

Os usuários devem receber acesso somente aos serviços que foram especificamente autorizados. O acesso de internet especificamente deve ser limitado ao mínimo de privilégio necessário para o usuário desempenhar suas atividades em Operação ou em Área de Apoio (Staff) e estes privilégios devem seguir um padrão para assegurar efetividade.

Os usuários que não estiverem em atividade devem ter seus acessos revogados.

Devem ser utilizados métodos apropriados de autenticação para controlar o acesso de usuários remotos.

O acesso aos sistemas operacionais deve ser controlado por diretrizes seguras de *log-on*.

Todos os usuários devem possuir um identificador único (user ID), de uso pessoal e intransferível e uma técnica de autenticação apropriada deve ser escolhida para confirmar a identidade do usuário.

As sessões devem ser finalizadas após o período de inatividade adequadamente determinado.

5.6. Gerenciamento de Incidente de Segurança da Informação

Os eventos de Segurança da Informação devem ser reportados o mais rápido possível através dos canais de comunicação apropriados.

Todos os colaboradores que utilizam os sistemas e serviços de informação devem ser conscientizados a reportar quaisquer fragilidades observadas ou suspeitas nestes recursos.

As diretrizes para notificar, coletar, retirar e apresentar evidências para o propósito de ações disciplinares devem ser estabelecidas e seguidas de acordo com a Política de Gestão de Incidentes de Segurança (PL-0039).

5.7. Gerenciamento da Continuidade do Negócio

Eventos que podem causar interrupções aos processos de negócio devem ser identificados juntamente com a probabilidade e o impacto de tais interrupções e suas consequências para a Segurança da Informação.

Planos devem ser desenvolvidos e implementados para manter ou restaurar as operações, assegurando a disponibilidade das informações no nível e no tempo requerido em caso de interrupção ou falha dos processos críticos de negócio.

Além disso, as diretrizes para a continuidade de negócio da Teleperformance Brasil devem ser seguidas conforme documento Política de Gestão Continuidade de Negócio (PL-0071).

5.8. Conformidade

Todos os requisitos estatutários, regulatórios e contratuais relevantes e a abordagem da Teleperformance Brasil diante destes elementos devem estar explicitamente definidos, documentados e atualizados para cada sistema de informação, conforme Política de Auditoria e Conformidade (PL-0083).

Devem ser implementadas diretrizes apropriadas para assegurar a conformidade com os requisitos legislativos, regulatórios e contratuais sobre o uso de materiais em respeito aos direitos de propriedade intelectual e sobre o uso de softwares proprietários.

Devem ser asseguradas a proteção e a privacidade dos dados conforme legislações, regulamentações e, se aplicável, cláusulas contratuais relevantes.

Os usuários devem ser impedidos de usar recursos de processamento de informações para propósitos não autorizados.

Os controles de criptografia devem ser usados em conformidade com todos os acordos, leis e regulamentações relevantes, conforme o documento Política de Gestão de Criptografias (PL-0065).

Os requisitos de auditoria e as atividades envolvendo análises em sistemas operacionais devem ser cuidadosamente planejados e acordados para minimizar o risco de comprometimento dos processos de negócio da empresa.

Os riscos oferecidos pelos processos de negócio que envolvam o ambiente devem ser identificados periodicamente, devendo ser implementados os controles apropriados conforme a Política de Gestão de Riscos da Segurança da Informação (PL-0042).

5.9. Contato com Autoridades e/ou Grupos Especiais

Devem ser mantidos os contatos necessários com as autoridades apropriadas para o suporte ao gerenciamento de incidentes de Segurança da Informação e ao processo de continuidade do negócio, bem como para antecipação e adequação a futuras mudanças em leis ou regulamentações.

Deve estar definido quando e por quem as autoridades devem ser contatadas e como os incidentes de Segurança da Informação devem ser reportados.

Devem ser mantidos contatos com grupos especiais, fóruns e associações profissionais relacionados à Segurança da Informação.

Além disso, a empresa possui o documento de Contato com Autoridades e Grupos Especiais (IT-0082), neste estão descritas as autoridades relevantes.

6. Penalidades

A utilização inadequada de recursos e/ou informação pode ser razão para aplicação de sanções administrativas por parte da Teleperformance Brasil, podendo, ainda, ocorrer demissão por justa causa nos termos do art. 482 da CLT ou rescisão de contrato de colaboradores.

7. Responsabilidades e Autoridades

Cargo	Responsabilidade	Autoridade
Todos	Conhecer, cumprir e aceitar com os requisitos desta política. Usar recursos de informação responsavelmente e em conformidade com as diretrizes	

	desta política e das citadas. Reportar qualquer suspeita de uso inapropriado de recursos de informação para seu gestor ou área de segurança da informação.	
Gestores	Assegurar que todos entenderam as políticas da empresa. Monitorar o uso de recursos de informação de seus colaboradores.	
Proprietário da Informação	Implantar medidas para proteger os recursos contra o uso inapropriado.	
Segurança da Informação	Estabelecer as diretrizes de segurança. Auditar o uso de recursos de informação da empresa a fim de assegurar a conformidade com políticas e instruções.	
Recursos Humanos	Gerenciar os processos de contratação, alteração e desligamento de colaboradores.	

8. Classificação do Documento

Uso Interno.

9. Registro de Revisões

Conforme registrado no sistema de controle de documentos.