

	ACESSO REMOTO	Emissão 14/10/2024	Classificação Uso interno
		Versão 1.09	Aprovado por: P!nk Corp Administration.
Código N-SI-008			

1. Introdução

- 1.1. A Norma de Acesso Remoto complementa a Política Geral de Segurança da Informação da P!NK CORP que oferece contratos de cartões de benefícios para empresas. Esta norma define diretrizes de segurança para o acesso remoto aos sistemas e dados corporativos, visando proteger os ativos de informação contra acessos indevidos e garantir a continuidade dos negócios.

2. Propósito

- 2.1. O propósito desta norma é assegurar que o acesso remoto aos ativos e serviços de informação seja realizado de maneira segura e controlada, prevenindo incidentes de segurança e protegendo os dados da empresa e de seus clientes.

3. Escopo

- 3.1. Esta norma aplica-se a todos os colaboradores, prestadores de serviços e terceiros autorizados a acessar remotamente os sistemas e dados da P!NK CORP.

4. Diretrizes

4.1. Concessão e Uso do Acesso Remoto

- 4.1.1. O acesso remoto será concedido somente a usuários que necessitem desse recurso para desempenhar atividades profissionais. É vedado o uso para fins pessoais ou outras atividades não relacionadas;
- 4.1.2. O usuário é responsável por toda e qualquer ação realizada com suas credenciais de acesso remoto, incluindo atividades não autorizadas realizadas por terceiros. O compartilhamento de credenciais é estritamente proibido;
- 4.1.3. O acesso remoto será configurado com os privilégios mínimos necessários para a execução das atividades do colaborador. Qualquer ampliação de privilégios deve ser justificada e aprovada pelo departamento de Segurança da Informação;

	ACESSO REMOTO	Emissão 14/10/2024	Classificação Uso interno
		Versão 1.09	Aprovado por: P!nk Corp Administration.

4.1.4. Dispositivos usados para acesso remoto devem possuir software de proteção contra códigos maliciosos (antivírus atualizado) e firewall ativo. O usuário deve garantir que o dispositivo esteja em conformidade com as diretrizes de segurança da P!NK CORP;

4.1.5. Em caso de perda ou roubo de dispositivos com acesso remoto habilitado, o usuário deve comunicar imediatamente a equipe de Segurança da Informação para que as medidas de proteção sejam acionadas.

4.2. Concessão e Uso do Acesso Remoto para Terceiros

4.2.1. O acesso remoto a terceiros só será concedido após a assinatura de um acordo de confidencialidade e em situações onde o acesso for essencial para a realização de atividades profissionais;

4.2.2. O período de acesso remoto concedido a terceiros será limitado ao tempo necessário para completar as atividades, não excedendo 30 dias corridos. Renovações do acesso devem ser justificadas e aprovadas pela Segurança da Informação;

4.2.3. Terceiros e a empresa prestadora de serviços são responsáveis por todas as ações executadas com as credenciais de acesso remoto fornecidas. Qualquer uso indevido deve ser comunicado imediatamente;

4.2.4. Equipamentos de terceiros com acesso remoto devem atender aos padrões de segurança, incluindo ferramentas de proteção contra malwares e firewall ativo;

4.2.5. Em caso de acesso não autorizado, perda ou roubo de dispositivos de terceiros, o incidente deve ser comunicado de imediato para a equipe de Segurança da Informação.

4.3. Monitoramento do Acesso Remoto

4.3.1. Todas as informações acessadas, transmitidas ou produzidas durante o acesso remoto estão sujeitas a monitoramento. O usuário deve estar ciente de que não há expectativa de privacidade no uso desse recurso;

	ACESSO REMOTO	Emissão 14/10/2024	Classificação Uso interno
		Versão 1.09	Aprovado por: P!nk Corp Administration.

4.3.2. A P!NK CORP reserva-se o direito de interceptar, registrar, copiar e monitorar qualquer atividade realizada durante o acesso remoto. Isso inclui atividades tanto de entrada (acesso à rede interna) quanto de saída (acesso a redes externas), assegurando a segurança e conformidade com as políticas corporativas.

5. Papéis e Responsabilidades

5.1. Gerência de Segurança da Informação:

5.1.1. É responsável por aprovar ou negar solicitações de acesso remoto, controlar e monitorar o uso do acesso remoto concedido e tratar incidentes relacionados ao uso indevido, comunicando-os ao Comitê Gestor de Segurança da Informação quando necessário.

5.2. Usuários do Acesso Remoto:

5.2.1. Devem utilizar o acesso remoto exclusivamente para fins profissionais, assegurar a segurança dos dispositivos e comunicar imediatamente qualquer incidente, como perda ou comprometimento de dispositivo e credenciais.

5.3. Prestadores de Serviço e Terceiros:

5.3.1. Devem garantir que os dispositivos usados para acesso remoto atendam às exigências de segurança e notificar qualquer evento de perda, roubo ou acesso não autorizado.

6. Sanções e Punições

6.1. O uso inadequado do acesso remoto, incluindo compartilhamento de credenciais, acesso indevido ou falha em relatar incidentes, poderá resultar em sanções conforme a Política Geral de Segurança da Informação. As penalidades incluem advertências, suspensão ou rescisão do contrato de trabalho ou de prestação de serviço, além de possíveis ações legais em casos de infrações graves.

	ACESSO REMOTO	Emissão 14/10/2024	Classificação Uso interno
		Versão 1.09	Aprovado por: P!nk Corp Administration.

7. Revisões

- 7.1. Esta norma será revisada anualmente pelo Comitê Gestor de Segurança da Informação para garantir que se mantenha atualizada com as melhores práticas de segurança e com as necessidades operacionais e de conformidade da P!NK CORP.

8. Gestão da Norma

- 8.1. A norma **N-SI-008** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria da P!NK CORP.
- 8.2. A presente norma foi aprovada no dia 14/10/2024