- **Controle de assinaturas e responsabilidades**

Versão	Data vigência	Responsável pela revisão	Responsável pela aprovação
00	15/09/2014	Gerente de TI	Diretor-Presidente
01	15/09/2015	Segurança da Informação	Diretor-Presidente
02	15/09/2016	Segurança da Informação	Diretor-Presidente
03	19/10/2016	Segurança da Informação	Diretor-Presidente
03	20/07/2016	Segurança da Informação	Diretor-Presidente
03	20/10/2016	Segurança da Informação	Diretor-Presidente
04	10/04/2018	Certificações e Métodos	Diretoria TI
05	12/03/2019	Certificações e Métodos	Diretoria TI
06	06/12/2019	Certificações e Métodos	Superintendência TI
07	02/04/2020	Certificações e Métodos	Superintendência TI

- **Controle de alterações**

Data revisão	Revisão	Descrição das alterações em relação à versão anterior
12/05/2014	00	▪ Não houve necessidade de alteração e/ou inclusão de novos itens
10/09/2014	01	▪ Atualização do item 4.3.1 Política de Mesa limpa e tela limpa, Sistemas de Informação e mídias, Controle aplicado, retirado disquetes e inserido Pen Drive ▪ Atualização do item 4.4.4 Acesso à Internet, retirada sugestão de envio de e-mail em caso de bloqueio de site.
15/07/2015	02	▪ Adicionado ponto 2.1 à política, fazendo menção as exceções de aplicação desta política.
15/07/2015	02	▪ Alterada modo de controle aplicado no item “Informação proprietária” (item 4.4.1), onde constava bloqueio do monitor em vez do sistema operacional da estação de trabalho
15/07/2015	02	▪ Adição de colaborador da área de Segurança da Informação dentro do grupo de participantes no comitê de SGI
15/07/2015	02	▪ Mencionado no item 4.4.3 o nível mínimo de complexidade para uso de senha do sistema operacional
15/07/2015	02	▪ Adicionada informação no tópico 4.4.5 Uso correto do correio eletrônico, restringindo o envio de mensagens com o conteúdo original alterado sem prévia autorização ou que a alteração seja mencionada na mensagem.

20/07/2015	02	▪ Adicionado novo tópico 4.4.4.2 Monitoramento CFTV, que contempla ciência sobre o monitoramento e normas de acesso para as imagens
25/08/2015	02	▪ Adicionado o campo 4.7.1.2. Revogação de acessos, mencionando a forma de efetuar os desligamentos e sua tempestividade
25/08/2015	02	▪ Adicionado o documento IOP-RH-009 nas referências
19/10/2016	03	▪ Adicionado “4.7.1.3. Revisão de acessos”, mencionando como é realizada a revisão dos acessos sistêmicos na PARLA!
20/07/2016	03	▪ Adicionado o Item 6, Revisão
20/10/2016	03	▪ Adicionado ao Item 4.7.1 descrições de matriz de acessos feitas pelo sistema GP e travas aplicadas ao mesmo. Item 4.4.1.1 foi atualizado com descrição de uso de dispositivos moveis. Inserido o controle 4.7.4. Acesso as Impressoras
10/04/2018	04	▪ Atualização do item 4.4.1 Política de Mesa limpa e tela limpa unificando informações proprietárias e pessoais
10/04/2018	04	▪ Adição de colaborador de Certificações e Métodos dentro do grupo de participantes no comitê de SGI
10/04/2018	04	▪ Atualização do Item 4.3.6 Acesso à internet
10/04/2018	04	▪ Inclusão “exceção clientes” no item 4.3.7
10/04/2018	04	▪ Atualização nomenclatura dos documentos de referência
12/03/2019	05	▪ Inclusão do item 3.1.2- referência a ISO 27001 ▪ Descrição incluída ao item 4.1.1 mencionando a ISO 27001 ▪ 4.3.1. Em controle aplicado, registrado a consideração de permissão ▪ 4.3.4. Em **NOTA 1**- Retirada a descrição de orientação para registro manual de controle de acesso ▪ 4.4.1 Alteração de análise crítica da PSI para 12 meses
06/12/2019	06	▪ Inserido no item 4.3.1 **Sistemas de informação e mídias** bloqueios aplicados na gestão e controle de dispositivos como PenDrives entre outros, descrito o controle aplicado na utilização de impressora quando permitido.
02/04/2020	07	▪ Acrescentado no item 4.10 descritivo referente ao HomeOffice
25/02/2021	08	▪ 3.5. Definições Incluídas as definições da LGPD. ▪ 4.5. Treinamento de Conscientização Incluído o treinamento obrigatório de LGPD a todos os colaboradores.

05/04/2021	09	▪ 4.4.1. CSI – Comitê de Segurança da Informação Incluída a DPO como membro obrigatório do CSI

1. Objetivo
Este documento tem por objetivo estabelecer as diretrizes, critérios e procedimentos adotados pela PARLA! para gestão da Política de Segurança da Informação.

2. Campo de aplicação
Este documento aplica-se a todas as áreas da PARLA!, bem como prestadores de serviços e terceiros.

2.1 Exceções ao uso desta política
Exceções sobre a aplicação destas políticas ficam sujeitas à contratos previamente acordados com clientes, contanto que não venham a ferir a segurança geral da companhia e de seus colaboradores. Não havendo exceção mencionada contratualmente e aprovadas pelo comitê de Segurança da Informação, esta política deverá ser aplicada em todo ambiente e para todos colaboradores PARLA!.

3. Definições
3.1. PCI DSS
Payment Card Industry Data Security Standard, ou, Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI).

3.1.2 ISO 27001
A Norma ISO 27001 é o padrão e a referência internacional para a gestão da segurança da informação

3.2. SI
Segurança da Informação

3.3. CSI
Comitê de Segurança da Informação

3.4. PCN
Plano de Continuidade de Negócios

3.5 Privacidade
Privacidade é o direito à reserva de informações pessoais e da própria vida pessoal. O direito ao respeito pela vida privada e familiar de uma pessoa, seu lar e sua correspondência. A Privacidade é o direito a ser protegido de uma interferência em assuntos pessoais;

3.6 Dados pessoais
Qualquer informação relativa a uma pessoa natural identificada ou identificável ('proprietário/titular/dono do dado'); uma pessoa natural identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador como nome, dados de identificação, dados de endereço, telefone, e-mail ou a um ou mais fatores específicos para a identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural. Dados pessoais podem incluir informações disponíveis sob qualquer forma: papel, texto, fotos, gráficos, vídeo, áudio, ou qualquer outro meio que leve à identificação do indivíduo de modo direto ou indireto;

3.7 Dado pessoal sensível
Origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político. Dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Dados sensíveis são somente aqueles que constam no Artigo 5º da Lei. Portanto, informações como salário ou dados de cartão de crédito, não são consideradas sensíveis perante à LGPD;

3.8 Titular dos Dados
Pessoa física a quem os dados fazem referência (exceção: pessoa falecida). Dono do Dado;

3.9 Dado anonimizado
Dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

3.10 Controlador: Responsável pelo Tratamento
Pode ser uma pessoa física ou jurídica, autoridade pública, agência ou outro organismo que determina os objetivos/finalidades e os meios do tratamento de dados pessoais;

3.11 Processador: Subcontratante
Pode ser pessoa física ou jurídica, autoridade pública, agência ou outro organismo que processe dados pessoais em nome do responsável pelo tratamento (Controlador);

3.12 Subprocessador
Terceiro Pessoa física ou jurídica que não seja o Titular de Dados, o Controlador ou o Processador e que esteja autorizada a processar dados pessoais;

3.13 Processamento
Qualquer operação ou conjunto de operações que seja realizada em dados pessoais ou em conjuntos de dados pessoais, seja por meios automatizados, como coleta, gravação, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, divulgação ou de outra forma disponibilização, alinhamento ou combinação, restrição, eliminação ou destruição;

3.14 Operador
Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

3.15 DPO
Data Protection Officer (Encarregado de Proteção de Dados)
Profissional que orienta a implementação de medidas apropriadas para compliance (conformidade/adequação legal) do controlador ou processador;

3.16 ANPD
Agência Nacional de Proteção de Dados - Órgão regulador da aplicação da lei.

4. Procedimentos, Responsabilidades e Abrangência

4.1. Introdução

A PARLA! desenvolveu um conjunto de controles, incluindo política, processos, estruturas organizacionais e procedimentos a fim de garantir a segurança de nossas informações e dos nossos clientes.

4.1.1. Objetivo

A Política de Segurança da Informação da PARLA! tem como objetivo garantir a confidencialidade, integridade e disponibilidade da informação no âmbito dos seus negócios.

Desta forma, o CSI da PARLA! se compromete a definir, estabelecer e implementar os requisitos da norma PCI DSS e ISO 27001 como boas práticas nos controles necessários para prevenir e reduzir os riscos de SI para nosso negócio, sempre em conformidade com as leis, normas, requisitos contratuais e procedimentos internos vigentes.

NOTA: Caberá ainda ao CSI garantir que a Política de SI seja comunicada e entendida a todas as partes interessadas.

4.2. Abrangência

A Política de Segurança da Informação abrange os aspectos de segurança físicos, lógicos, de informação, de pessoas e da imagem da PARLA!.

4.3. Diretrizes Gerais de Segurança da Informação

4.3.1. Política de mesa limpa e tela limpa

Todos os colaboradores, prestadores de serviços e terceiros que atuam nas áreas operacionais e administrativas devem praticar e orientar conforme os seguintes controles:

Tipo	Violação	Risco	Controle aplicado
Informações proprietárias/ pessoais	Agendas, cadernos, cartões de visitas, objetos pessoais sobre a mesa.	Informações pessoais e profissionais - incluindo números de telefone, senhas e anotações em geral - estão vulneráveis.	▪ **Quando permitido**, guarde agendas, cadernos de anotações, cartões, objetos pessoais em gaveta/armário trancado ou leve-as consigo ao deixar sua mesa por longos períodos.
Ferramentas de acesso	Chaves, telefone celular, notebook e o crachá de acesso sobre a mesa.	Celulares e notebooks podem ser roubados ou ter seus históricos comprometidos. Chaves roubadas dão a intrusos acesso a áreas restritas. Notebook contém dados sensíveis pessoais e profissionais. Crachás roubados podem ser usados para acesso indevido.	▪ Mantenha os equipamentos com você e trave celulares e notebook com senhas; ▪ Utilize o cadeado para notebook quando se ausentar da estação de trabalho; ▪ Nunca deixe seu crachá ou chaves em qualquer lugar; mantenha-as junto a você; ▪ Notifique o DP imediatamente se seu crachá sumir ou ao ADM em caso de perda das chaves.
Sistemas de informação e mídias	Aplicativos abertos no computador, computador desbloqueado, senha anotada no post-it colado no suporte do monitor, documentos impressos na impressora.	Acesso as mensagens eletrônicas (pessoais ou corporativas) ou senhas podem permitir intrusão. Os CDs no drive e informações nos documentos impressos podem ser roubados. Arquivos *cache* de aplicativos e impressoras podem conter dados sensíveis e difíceis de serem preservados.	▪ Bloqueie o sistema operacional do computador quando deixar sua mesa; ▪ Não deixe mídias, como CDs ou pen drives no computador; ▪ **Por padrão é aplicado em nossos equipamentos o bloqueio de acesso a dispositivos como os mencionados acima** ▪ Utilize o protetor de telas protegido por senha; ▪ Desligue seu computador quando sair da sala por longos períodos; ▪ Nunca escreva senhas em lembretes; ▪ **Quando permitido**, Retire os documentos assim que imprimi-los; ▪ **Por padrão a utilização da impressora é controlada via software de gerenciamento de impressões.** ▪ Destrua impressos sensíveis após usá-los; ▪ Limpe arquivos de *cache* regularmente.

Ferramentas de acesso	Computadores e informativos posicionados frente a janelas e corredores com dados sensíveis em ângulo visível.	A exposição poderá permitir a espionagem e acesso não autorizado a dados sensíveis.	▪ Computadores e informativos deverão ser posicionados de forma que dados sensíveis não sejam visíveis de janelas ou corredores;
Além da mesa de trabalho	Gaveta de pastas suspensas abertas e as chaves na fechadura. Cesto de lixo com papéis não destruídos. Prateleira de livros com pastas contendo informação sensível.	Visualização ou extravio de documentos sensíveis podem ser extraídos em horários fora do expediente ou recuperados no depósito fora da empresa. As pastas na prateleira, claramente marcadas como sensíveis, também são passíveis de extravio de informação e, portanto, de difícil detecção.	▪ Não guarde pastas com documentos sensíveis na prateleira. Marque-as de forma normal e tranque-as; ▪ Faça um arranjo na gaveta de pastas suspensas de forma a manter pastas menos sensíveis na frente e mais sensíveis na parte de trás; ▪ Mantenhas as gavetas fechadas/trancadas e não deixe as chaves na fechadura; ▪ Destrua os documentos impressos antes de jogá-los fora ▪ Tranque sua sala ao deixá-la por longos períodos.

Adicionalmente, são adotados controles específicos para áreas onde são processadas informações classificadas como “confidencial” e “restrita” e que impactam diretamente na segurança da informação dos nossos clientes e no diferencial competitivo da PARLA! que constam no item 4.11.

4.3.2. Ambiente Operacional

É proibido o uso de dispositivos móveis e de meios físicos para extração de informação, tais como: aparelhos celulares, máquinas fotográficas, *pen drives*, papeis em geral (cadernos, agendas, bloco de notas e etc.) e canetas nos ambientes onde atuam operadores, monitores e supervisores operacionais.

A concessão para uso de dispositivos móveis aos funcionários é permitida nos níveis de diretor, superintendentes, gerentes executivos e gerentes, coordenadores que estejam em pleno exercício de suas funções e que tenham recebido os equipamentos de titularidade PARLA!. Aos demais funcionários a concessão estará sujeita à aprovação do Setor de Segurança da informação, superintendente da área e diretoria.

Para maiores informações sobre o gerenciamento para uso de dispositivos móveis no âmbito da PARLA!. deve-se consultar o PR-TI-001 – Diretrizes para gerenciamento de acessos lógicos e recursos tecnológicos.

Nos ambientes operacionais é permitido a entrada somente da garrafa de água e materiais de treinamento fornecidos pelos clientes quando necessário.

Caberá a área de Segurança da Informação realizar inspeções periódicas nos ambientes operacionais a fim de constatar a conformidade com as diretrizes acima descritas.

NOTA 1: Externamente ao ambiente operacional são disponibilizados armários individuais para guardar os pertences dos colaboradores que atuam nestes ambientes.

NOTA 2: O não cumprimento das diretrizes descritas nos itens 4.3 e subitens por qualquer colaborador implicará em sanção disciplinar conforme processo disciplinar vigente ou prestadores de serviços e fornecedores na reavaliação de contratos de prestação de serviços.

4.3.3 Monitoramento CFTV

A companhia é monitorada 24 horas por dia, sete dias por semana através de um sistema CFTV (Circuito fechado de televisão), incluindo ambientes operacionais, tecnológicos e administrativos.

As imagens obtidas pelo sistema são armazenadas internamente, somente sendo acessíveis pela área de Administração Predial, Segurança da Informação e pela área de Tecnologia da Informação.

Em casos de auditoria ou demais necessidades de acesso às imagens gravadas, deverá ser solicitado à área de Segurança da Informação através de abertura de chamado em ferramenta interna. A liberação destas imagens dependerá da aprovação da Gerencia Executiva da área solicitante e da Gerencia Executiva de TI, sendo enviadas ao gerente responsável da área solicitante.

4.3.4. Uso correto de crachás

O controle de acesso físico as dependências internas da PARLA! são garantidas, entre outros controles, por meio do crachá de acesso e identificação que é fornecido para todos os colaboradores, clientes, visitantes e prestadores de serviço envolvidos em nossas atividades. Estes serão registrados para o monitoramento periódico de conformidade das regras.

Para o uso correto do crachá deverão ser adotadas as seguintes regras:

- O crachá é único, pessoal e intransferível, logo todo acesso será atribuído ao seu usuário;
- Utilizar o crachá de maneira visível enquanto estiver dentro das dependências físicas da PARLA!;
- Não é permitido emprestar o crachá de acesso;
- Não permitir a entrada ou entrar em áreas controladas de “carona”, tais como, ambiente operacional, ambiente de desenvolvimento de sistemas, datacenter e entre outras.

NOTA 1: Todo usuário portador de crachá deverá registrar sua movimentação física nas dependências da PARLA!.
Para maiores detalhes sobre o controle de acesso e segurança física deve-se consultar o item 4.8.

4.3.5. Gestão de senhas

Para cada acesso lógico aos sistemas ou recursos tecnológicos da PARLA! é disponibilizada uma senha de identificação para o usuário autorizado (ver item 4.6).

Cabe a cada colaborador praticar as seguintes diretrizes de segurança para uso de senhas:

- A senha de identificação é única, pessoal e intransferível, logo o usuário não deve compartilhá-la com outros colaboradores;
- O usuário deve trocar sua senha de acesso aos recursos periodicamente, conforme as diretrizes adotadas pela PARLA!;
- Não elaborar senhas com números sequenciais (ex.:1234) ou aspectos pessoais, tais como, data de nascimento e sobrenomes;
- O usuário não deve utilizar o recurso de “lembrar senhas” nos sistemas e recursos tecnológicos da PARLA!.
- A senha do colaborador deve conter um nível mínimo de complexidade, contendo no mínimo 8 caracteres, dentre eles letras, ao menos um número e caracteres especiais (! @, #, $% etc.)

A senha de identificação qualifica o usuário como responsável por todos os acessos realizados. A definição e a utilização de senhas estão condicionadas às regras definidas pela área TI, em conjunto com o CSI.

4.3.6 Acesso à internet

Uma vez criada a conta, o colaborador não terá acesso a sites que tenham o seguinte conteúdo:

- Pornografia;
- Jogos;
- Bate papo;
- *Webmail;*
- *Instant Messenger;*
- Busca de softwares de código aberto, piratas e downloads;

- Redes sociais e relacionamentos;
- Outros que o CSI venha a determinar como restritos.

NOTA:
A restrição é garantida na área TI, por meio de filtros de conteúdo que entram em ação na solicitação do cliente ao site, conforme definição do perfil na autenticação do usuário no servidor. Ao tentar o acesso a um site com conteúdo restrito o usuário será impedido e receberá uma mensagem restritiva.

4.3.7 Uso correto do correio eletrônico

A conta de correio eletrônico disponibilizada pela PARLA! é de uso exclusivamente profissional e caberá a área de TI realizar toda gestão de uso de correio eletrônico. O usuário é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail.

Lembrando que, a empresa poderá a qualquer tempo monitorar o recebimento e envio de mensagens de seus colaboradores e partes envolvidas (exceto clientes), sendo que é proibido criar, copiar ou encaminhar mensagens ou imagens que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
- Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;
- Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a PARLA!, a sugestão deve ser encaminhada para a Área de Recursos Humanos, que definirá a sua publicação ou não;
- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
- Sejam hostis ou transmitam indiretamente mensagens hostis;
- Defendam ou possibilitem a realização de atividades ilegais;
- Possam prejudicar a imagem da PARLA!, parceiros e clientes.
- Alterar o conteúdo original de mensagens e repassar as mesmas sem fazer menção desta alteração. A modificação do conteúdo original de mensagens realizada sem prévia autorização pode ser caracterizada como fraude e esta ação será tratada judicialmente conforme os parâmetros das leis vigentes.

4.4. Responsabilidades

4.4.1. Comitê de Segurança da Informação - CSI

É função do Comitê de Segurança da Informação estabelecer as responsabilidades gerais e específicas na gestão de segurança da informação, bem como estabelecer diretrizes e oferecer suporte às iniciativas de segurança da informação.

Cabe ao CSI:

- Revisar e recomendar aprovação das políticas, normas e procedimentos gerais relacionados à segurança da informação;
- Realizar a análise crítica da Política de Segurança da Informação, no mínimo a cada doze (12) meses e apresentar a sua conclusão para aprovação da diretoria;
- Aprovar as principais iniciativas para a melhoria contínua das medidas de proteção;
- Apoiar a implantação de soluções para eliminação ou minimização dos riscos;
- Estabelecer uma relação consistente das estratégias de negócios e da Tecnologia da Informação com os aspectos de segurança;
- Suportar perante toda a PARLA! as iniciativas de Segurança da Informação.

Caso ocorram eventos ou fatos relevantes uma reunião imediata poderá ser convocada pela coordenação do CSI que terá, entre outras, tal responsabilidade.

NOTA: Em todos os casos, devem-se registrar as saídas das reuniões no FOR-CORP-001 – Ata de reunião e arquivá-las conforme disposição descrita no item 4.

O quadro abaixo representa a estrutura atual do CSI da PARLA!, sendo que a coordenação do CSI é de responsabilidade do gerente da área de TI.

Cargo / Função	Área atuação	Participação no CSI
Gerente	Tecnologia da Informação	Obrigatória
Analista	Segurança da Informação	Obrigatória
Diretor	Administrativo	Obrigatória
Diretor	Operacional	Obrigatória
Gerente	Recursos Humanos	Facultativa
Gerente	Departamento Pessoal (jurídico)	Facultativa
Gerente	Certificações e Métodos	Obrigatória
DPO	Tecnologia da Informação	Obrigatória

Outras áreas poderão ser convocadas às reuniões de acordo com o assunto a ser tratado.

4.4.2. Cumprimento das regras
Caberá a todos os colaboradores da PARLA! envolvidos:

- Observar e fazer cumprir todas as diretrizes gerais de Segurança da Informação da PARLA!;
- Comunicar imediatamente o CSI, em caso de incidente de SI conforme item 4.9.

NOTA: Em caso de um colaborador violar / não cumprir as diretrizes gerais de segurança da informação, o mesmo estará sujeito à aplicação de sanções disciplinares definidas pela PARLA!.

4.4.3. Área Tecnologia da Informação
Caberá à área de Tecnologia da Informação da PARLA!, entre outras atividades, as seguintes responsabilidades:

- Definir, em articulação com o CSI, as diretrizes de segurança da informação a serem adotadas nos ambientes de tecnologia da informação da PARLA!;
- Administrar a infraestrutura de tecnologia da informação de forma a garantir os requisitos necessários para preservar a segurança das informações;
- Implantar controles efetivos para concessão, revisão e exclusão, bem como para o monitoramento diário do uso correto dos acessos lógicos e dos recursos tecnológicos da PARLA!.

4.4.4. Lideranças
A responsabilidade das lideranças da PARLA! para com a segurança da informação compreende as seguintes atividades:

- Gerenciar o cumprimento da Política de Segurança da Informação, por parte de seus colaboradores e prestadores de serviços;
- Garantir que o pessoal sob sua gestão compreenda e desempenhe o seu papel dentro do CSI;
- Comunicar imediatamente o CSI, em caso de incidente de SI que, eventualmente, possa ocorrer em sua área.

4.4.5. Fornecedores
Caberá a área Comercial em conjunto com os interessados, garantir quando aplicável, que estarão previstas no instrumento do contrato as cláusulas que contemplem a responsabilidade dos fornecedores no cumprimento da Política de Segurança da Informação, além das normas e procedimentos internos vigentes.

As atividades de contratação, qualificação e avaliação de fornecedores e prestadores de serviços de temas específicos estão no processo documentado PR-FI-001 - Processo de qualificação e avaliação de fornecedores.

4.4.6. Jurídico
Caberá a área Jurídica da PARLA!, dentre outras responsabilidades, as seguintes atividades:

- Auxiliar o CSI quanto aos aspectos legais, requisitos regulamentares e contratuais;
- Auxiliar na avaliação dos incidentes de SI causados por funcionários, prestadores de serviços e terceiros aplicando as sanções disciplinares cabíveis, leis trabalhistas, bem como a reavaliação de contratos de prestação de serviços;
- Elaborar e aplicar, quando necessário, "acordo de não divulgação" entre a PARLA! e partes terceiras envolvidas (clientes e fornecedores).

4.4.7. Gestor de Contratos
Caberá ao gestor de cada contrato, dentre outras responsabilidades, as seguintes atividades:

- Manter uma relação atualizada dos prestadores de serviço, conforme definido no PR-FI-001 - Processo de qualificação e avaliação de fornecedores;
- Realizar a avaliação do prestador de serviço quanto ao atendimento aos requisitos e diretrizes de segurança da informação da PARLA!.

4.5. Conscientização e Treinamento
Como forma de garantir que os funcionários, terceiros e prestadores de serviço tenham recebido informações necessárias para cumprir de maneira correta com as diretrizes da Política de Segurança da Informação são realizados treinamentos e reciclagens em todo escopo da PARLA!.

Além disto, todos os colaboradores que atuam no escopo da PARLA! assinam o termo de sigilo e confidencialidade na efetivação dos seus contratos.

Como forma de se manter um processo contínuo de conscientização dos colaboradores, são utilizados murais e quadros estrategicamente localizados para a divulgação das regras de segurança da informação da PARLA!, além da divulgação na intranet.

Além disto, são desenvolvidas campanhas pelo CSI, em conjunto com a área de RH da PARLA!, para que sejam realizados, no mínimo, treinamentos anuais sobre das diretrizes de segurança junto aos colaboradores.

NOTA: Os treinamentos de reciclagens poderão ser realizados em intervalos menores com o objetivo de disseminar novas diretrizes e práticas de segurança da informação ligadas ao negócio da PARLA!, tais como requisitos contratuais de clientes. Como no caso da LGPD, cujo treinamento é obrigatório a todos os colaboradores da Parla!, incluindo a direção, com periodicidade prevista de realização anual.

Para realização do planejamento de conscientização e treinamento dos nossos colaboradores (funcionários, prestadores de serviços e terceiros) nas diretrizes de Segurança da Informação e registro destas ações deve-se proceder conforme o PR-RH-001 - Processo de gestão de pessoas.

4.6. Acessos lógicos e recursos tecnológicos
Os privilégios de acesso na PARLA!! estão definidos de acordo com atuação de cada tipo de usuário/cargo existente (funcionários, clientes, terceiros e prestadores de serviços).

Os níveis de acesso estão determinados de acordo a matriz de alçadas de autorização elaborada e aprovada pelo CSI. Esta matriz é feita e controlada pelo Sistema GP (Gestão de Pessoas), a qual possui travas que não permitem que colaboradores alterem registros ou possam realizar auto aprovação em perfis de acesso ou qualquer circunstância que possa gerar alto favorecimento sem a aprovação de sua Gestão Direta, ou em alguns casos, do setor de Segurança da Informação.

O documento PR-TI-001 – Diretrizes para gerenciamento de acessos lógicos e recursos tecnológicos descreve todas as atividades de gerenciamento de acessos lógicos que envolvem os acessos à rede,

sistemas de informação, internet e correio eletrônico, além do controle de uso de softwares, acesso remoto, redes sem fio e para uso de dispositivos móveis.

4.6.1. Controles de acesso à rede e sistemas de informação
O acesso à rede interna da PARLA! e aos seus diversos sistemas de informação estão limitados aos colaboradores devidamente autorizados conforme item mencionado acima, 4.6.

As solicitações para inclusão, revisão e exclusão de acessos à rede e sistemas de informação são direcionadas para a área de TI da PARLA!. Caberá a área TI executar a gestão de acessos a fim de garantir o cumprimento das diretrizes de segurança lógica da PARLA!.
A utilização de dispositivos físicos como notebooks e entre outros de titularidade de clientes, fornecedores ou visitantes são delimitados ao uso da rede via WIFI – Externa com restrição de zona da rede local, permitindo o acesso para internet apenas através de autenticação com login pessoal.

4.6.1.2. Revogação de acessos
A revogação de acessos dos colaboradores desligados da companhia deve ser realizada tempestivamente, tendo como tempo máximo 24 horas após o desligamento do ex-colaborador. A revogação dos acessos é solicitada através do sistema GP (Gestão de Pessoas). Para casos de exceções, deverá ser avaliado o documento IOP-RH-009 – SOLICITAÇÃO DE DESLIGAMENTO, seguindo suas imposições descritas.

4.6.1.3. Revisão de acessos
A revisão dos acessos é realizada através de Controles Internos que a área de Tecnologia da Informação e as gestões operacionais realizam, passando pela validação da área de Segurança da Informação. As informações de funcionamento destes controles bem como sobre os seus devidos formulários estão documentadas em IOP-TI-002 - Diretrizes para Administração de Acessos Lógicos.

4.6.2. Controle de uso de softwares
Para evitar a utilização de softwares não autorizados, homologados e/ou licenciados legalmente, apenas a área TI está autorizada a realizar a instalação de ativos de softwares na PARLA! desde que esteja autorizado e descrito em procedimento interno.

4.6.3. Acesso remoto e redes sem fio
A utilização de acessos remotos por meio de qualquer método é somente para usuários devidamente autorizados, bem como o acesso à rede sem fio no ambiente da PARLA! somente será permitido aos usuários com acessos lógicos e dispositivos móveis autorizados (visitantes ou clientes).

4.6.4. Acesso às Impressoras
A informação impressa representa um risco a informação, e mediante a isso a PARLA! realiza a restrição de acesso as impressoras mediante a função de cada colaborador. O acesso é liberado apenas para supervisores, coordenadores, Gerentes, TI, Segurança da Informação e Diretor/Presidência da Empresa, salvo restrições contratuais.

O controle e gestão de acesso é feito por software de gerenciamento de impressão, onde mensalmente é liberado um valor previamente definido por cargo para que o colaborador possa fazer uso da Impressora. Para maiores Informações sobre procedimentos relacionados, favor consultar o documento IOP-TI-002 - Diretrizes para Administração de Acessos Lógicos.

NOTA1: Documentos Impressos, bem como as informações descritas neste, são de responsabilidade do responsável pela impressão. Informação de caráter confidencial deixadas nas impressoras, por qualquer colaborador, prestadores de serviços ou terceiro implicará em sanção disciplinar conforme processo disciplinar vigente ou na reavaliação de contratos de prestação de serviços.

NOTA2: Exceções deverão ser avaliadas em comitê de CSI e deverão ter aprovação da Diretoria da PARLA!.

4.7. Gestão de ativos e gerenciamento de riscos de segurança da informação
A PARLA! adota uma gestão segura sobre seus ativos de SI, sendo assim garante que os mesmos são inventariados, classificados, atualizados periodicamente e principalmente que possuam um gestor responsável formalmente designado.

O processo de gerenciamento de riscos, que inclui a análise e avaliação de riscos é analisado criticamente, no mínimo a cada doze (12) meses, pelo Comitê de Segurança da Informação (CSI). A análise crítica deverá ser realizada como forma de prevenção contra riscos, inclusive aqueles oriundos de novas tecnologias, visando à elaboração de planos de ação apropriados em virtude das ameaçadas identificadas.

Para maiores detalhes da descrição da metodologia aplicada para realização do controle de ativos, da análise e avaliação de risco, dos critérios para a aceitação de risco, bem como da identificação dos níveis aceitáveis de risco, deve-se consultar a PR-SI-002- Diretrizes para gestão de ativos de segurança da informação e gerenciamento de riscos**.**

4.8. Controle de acesso físico
As áreas seguras e protegidas da PARLA! são protegidas por perímetros de segurança (recepções, catracas, leitores de crachá e leitor biométrico) e por um sistema apropriado, que permite a entrada e saída apenas de pessoas nos respectivos setores autorizadas.

Os níveis de acesso estão determinados de acordo com a matriz de alçadas de autorização elaborada e aprovada pelo CSI e pela Diretoria.

Todas as solicitações para inclusão e revisão de acessos físicos dos colaboradores são direcionadas para a área de TI da PARLA!, sendo que caberá a área TI executar a gestão de acessos a fim de garantir o cumprimento das diretrizes de segurança física da PARLA!.

A remoção de acessos físicos para os colaboradores será realizada quando da efetivação do seu desligamento pelo sistema de gestão de pessoas da PARLA! ou quando solicitado.

Cabe a cada colaborador, prestador de serviço ou cliente da PARLA! seguir as seguintes diretrizes de acesso físico:

- Respeitar os acessos definidos e concedidos a sua função/cargo;
- Não permitir a entrada de pessoas não autorizadas em seu local de trabalho (salvo nos casos que a solicitação for autorizada);
- Zelar pela segurança física garantindo o fechamento adequado de portas e demais controles acessos às áreas;
- Comunicar imediatamente qualquer caso de incidente de SI relacionado aos aspectos de segurança física.
- Informar sua gestão em caso de perda ou extravio de seu crachá;

NOTA: O colaborador que acessar uma área não autorizada (segura) estará sujeito à aplicação de sanções disciplinares definidas pela PARLA! e nos casos de prestadores de serviços terem seus contratos reavaliados ou mesmo cancelados.

Para maiores informações sobre o controle dos acessos físicos e a segurança dos equipamentos da PARLA! deve-se consultar a PR-SI-003 – Diretrizes de controle de acesso e segurança física.

4.9. Gerenciamento de Incidentes de Segurança da Informação
Os incidentes de segurança que envolve os escopos de atuação da PARLA! devem ser reportados diretamente para a área de Tecnologia da Informação.

As diretrizes de respostas a incidentes, as responsabilidades, a capacitação das equipes envolvidas, bem como a realização dos testes periódicos e a comunicação junto as partes envolvidas estão descritas no documento PR-SI-004 - Gestão de Incidentes de Segurança da Informação.

4.10. Plano de continuidade de negócios

O plano de continuidade de negócios da PARLA! visa estabelecer o planejamento de ações que são adotadas em uma eventual situação de crise, possibilitando continuar nossas atividades de negócio em um nível aceitável definido pela Alta Direção.

O escopo do PCN da PARLA! abrange os aspectos físicos, lógicos, de recursos humanos e legais da área Tecnologia da Informação, sendo que o PCN é composto do plano de administração de crises e do plano de continuidade e recuperação de desastres.

Em empresas de Contact Center o trabalho em site físico sempre foi pré-requisito em virtude de confidencialidade de dados e sistemas além de diversos parâmetros de segurança de informações.

Estruturamos nossas plataformas operacionais e sistemas de controle para atuação em Home Office e reorganizamos os modelos de condicionamento de nossos colaboradores dentro do nosso site.

Atualmente temos 50% dos colaboradores trabalhando em formato Home Office e os que permanecem atuando em nosso site, por determinação de nossos demandantes, contam com infraestrutura apropriada para garantir total segurança em sua jornada de trabalho.

Possuímos estrutura de processos para suporte aos nossos colaboradores que estão trabalhando em modelo Home Office por meio de chat para o qual uma equipe de TI é responsável pelo atendimento dos casos dentro da fila de demanda gerada pelos nossos colaboradores.

Esse atendimento possui algumas formas de tratativa desde ser tratado e encerrado em ambiente do Chat ou até mesmo o compartilhamento de tela frente a uma necessidade de suporte mais especifica.

Em casos excepcionais em que a modalidade Home Office não se enquadre por qualquer motivo, nossa sede dispõe de 2 prédios, onde já temos um como contingência do outro. Adicionalmente na impossibilidade de realizar operações devido à incêndio e demais incidentes na sua sede, à Avenida Tamboré, nº 350 – Tamboré – Barueri – SP e segundo as estratégias definidas no Plano de Recuperação de Desastres, a Contingência externa será realizada em site terceiro contratado, situado na Av. Maria Coelho Aguiar, 215 – São Paulo, SP, onde existem cópias dos servidores do site principal permitindo retorno parcial da operação em caso de emergência a depender do modelo de contrato instituído com o cliente.

NOTA: Um plano de continuidade e recuperação de desastres para a área operacional poderá ser elaborado, implantando e testado conforme exigência contratual dos nossos clientes.

As atividades que envolvem o gerenciamento do Plano de continuidade de negócios estão descritas no documento PR-SI-005 – Diretrizes do Plano de continuidade de negócios.

4.11. Classificação e rotulação das informações

4.11.1. Classificação

Todos os ativos de informação deverão ser classificados conforme a sua criticidade para a PARLA!. Caberá ao CSI, em conjunto com as lideranças das áreas aplicarem a seguinte classificação para as informações:

Informação Pública: É toda informação que pode ser acessada por todos os colaboradores, clientes, prestadores de serviços e público em geral.

Informação Interna: É toda informação que só pode ser acessada por colaboradores. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

Informação Confidencial: É toda informação que pode ser acessada por usuários da PARLA! e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio dos seus clientes.

Informação Restrita: É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e comprometer a estratégia de negócio da PARLA! e a segurança da informação dos nossos clientes.
As atividades envolvidas para solicitação de autorização de divulgação, bem como o tratamento aplicado para informações classificadas como interna, confidencial e restrita estão descritas no documento IOP-SI-001 – Diretrizes para Classificação e Tratamento das Informações.

4.11.2. Rotulação
A rotulação das informações é de responsabilidade de todos os colaboradores da PARLA!. Para os documentos da PARLA! a rotulação é realizada conforme documento PR-CP-001- Diretrizes para Controle de Documentos e Registros.

NOTA: A cópia ou divulgação não autorizada de informações classificadas como de uso restrita, confidencial e interna são expressamente proibidas sob pena de processo civil ou criminal, além da aplicação das leis trabalhistas.

5. Controle de registros

1. Identificação do Nome / Código dos Registros	2. Restrições de Acesso / Proteção	3. Definição da Disposição a ser dada ao Registro	4. Ordenamento / Indexação Ativo	5. Tempo de Retenção Ativo	6. Ordenamento / Indexação Inativo	7. Tempo de Retenção Inativo
FOR-CORP-001 – Ata de reunião do CSI	CSI+CP	Manter em arquivo **ativo** permanentemente	Por data	Permanentemente	Não aplicável	Não aplicável

6. Revisão

Este documento deverá ser revisado a cada 12 meses, a partir de sua publicação.

7. Documentos de referência

PR-TI-001 - Diretrizes para gerenciamento de acessos lógicos e recursos tecnológicos
IOP-SI-001 - Diretrizes para Classificação e Tratamento das Informações
PR-SI-002- Diretrizes para gestão de ativos de segurança da informação e gerenciamento de riscos
PR-SI-003 - Diretrizes de controle de acesso e segurança física
PR-SI-004 - Gestão de Incidentes de Segurança da Informação
PR-SI-005 - Diretrizes do Plano de continuidade de negócios
PR-SI-007- Diretrizes para classificação e tratamento das informações
IOP-TI-002 - Diretrizes para Administração de Acessos Lógicos.
IOP-RH-009 - Solicitação de desligamento
PR-RH-001 - Processo de gestão de pessoas
PR-CP-001- Diretrizes para Controle de Documentos e Registros
PR-FI-001 - Processo de qualificação e avaliação de fornecedores
FOR-CORP-001- Ata de reunião