Bellinati Perez

Documento Público

Política Corporativa de Segurança da Informação	
Código: 01 **Versão: 6.2** **Criação:** 30/09/2020 | **Revisão:** 08/12/2023 **Tipo de Documento:** Público	Bellinati Perez

1. OBJETIVOS COM ESCOPO E PROPÓSITOS

Esta política tem por objetivo estabelecer critérios e diretrizes relativas à Segurança da Informação, no que tange a utilização de dados e informações nos processos de negócio da **Bellinati Perez**.

A segurança da informação da Bellinati Perez, tem como objetivo proteger os dados pessoais e financeiros dos seus clientes, dos seus funcionários e de seus fornecedores, bem como as informações estratégicas e operacionais da empresa, contra ameaças internas e externas, como invasões, vazamentos, fraudes, sabotagens etc.

A segurança da informação visa garantir a confidencialidade, a integridade, a disponibilidade, a autenticidade e a legalidade dos dados e das informações.

Os principais objetivos da segurança da informação são:

- Confidencialidade: significa que os dados e as informações só devem ser acessados por pessoas autorizadas, evitando o acesso indevido ou a divulgação não consentida;
- Integridade: significa que os dados e as informações devem ser mantidos íntegros, sem alterações, perdas ou danos, durante o seu armazenamento, processamento ou transmissão;
- Disponibilidade: significa que os dados e as informações devem estar disponíveis para os usuários autorizados sempre que necessário, sem interrupções ou atrasos;
- Autenticidade: significa que os dados e as informações devem ser verificáveis quanto à sua origem, identidade e validade, evitando falsificações ou adulterações;
- Legalidade: significa que os dados e as informações devem ser tratados de acordo com a legislação vigente, respeitando os direitos e deveres dos titulares, dos controladores e dos operadores.

Para alcançar esses objetivos, a Bellinati Perez adota medidas técnicas, administrativas e educacionais de segurança da informação, tais como:

- Criptografar os dados sensíveis, tanto em repouso quanto em trânsito, usando algoritmos e chaves seguras.
- Usar senhas fortes, complexas e únicas para cada sistema ou serviço, e trocá-las periodicamente.
- Implementar um sistema de controle de acesso, baseado nos princípios do menor privilégio e da necessidade de saber, definindo perfis, papéis e permissões para cada usuário.
- Realizar backups regulares dos dados críticos, e armazená-los em locais seguros e distintos.
- Instalar e atualizar softwares de proteção, como antivírus, firewall, antimalware, etc., em todos os dispositivos e redes da empresa.
- Monitorar e auditar as atividades e os eventos de segurança da informação, registrando e analisando os logs, alertas e incidentes.
- Elaborar e revisar políticas, normas e procedimentos de segurança da informação, alinhados com as boas práticas e os padrões do mercado.
- Conscientizar e capacitar os funcionários e os parceiros sobre a importância e as boas práticas de segurança da informação, realizando treinamentos, campanhas e testes.
- Avaliar e gerenciar os riscos de segurança da informação, identificando as ameaças, as vulnerabilidades e os impactos, e definindo as ações de prevenção, mitigação e recuperação.

A **Bellinati Perez** engajou programas para um Sistema de Gestão de Segurança da Informação (SGSI), e para um Sistema de Gestão de Privacidade da Informação (SGPI), que estão alinhados às normas internacionais ISO/IEC 27001:2013 e ISO/IEC 27701:2019, para garantir que os processos de informações pessoais sejam conduzidos pautados em uma rígida Gestão de Riscos de Segurança e Privacidade, e demais boas práticas de governança de serviços e de dados.

O propósito desta política é atender aos requisitos legais, regulatórios e contratuais que envolvem a organização **Bellinati Perez,** e assim atender as questões internas e externas que são relevantes para a organização e que afetam a sua capacidade de alcançar os resultados pretendidos do SGSI e SGPI, bem como pautadas por meio de um processo de análise de riscos.

A **Bellinati Perez** possui processo de análise de riscos que envolvem as seguintes etapas:

Identificação dos ativos de informação:

A **primeira etapa** identifica os ativos de informação da organização, ou seja, os dados e sistemas que são importantes para o negócio:

- Dados: Dados dos titulares inadimplentes, dados do contrato de financiamento ou compra de produtos, bem como dados dos seus colaboradores, clientes e fornecedores.
- Sistemas: CRM's utilizados pela operação, e Sistemas utilizados pelo Backoffice, Departamento Pessoal e RH.

Identificação das ameaças:

A **segunda etapa** é identificar as ameaças que podem afetar os ativos de informação da organização – Incidentes de Segurança, Ataques de Ransomware, Falhas de Hardware e de Software.

Avaliação da probabilidade e impacto das ameaças:
A **terceira etapa** é avaliar a probabilidade e o impacto de cada ameaça.

Determinação dos controles:
A **quarta etapa** é determinar os controles que podem ser implementados para mitigar os riscos identificados.

Ferramentas e métodos para análise de riscos:

- Avaliação de risco por pares:
  Esta ferramenta envolve um grupo de especialistas que avaliam os riscos de forma colaborativa.
- RACI (Responsible, Accountable, Consulted, Informed):
  Esta ferramenta é utilizada para atribuir responsabilidades para as atividades de gerenciamento de riscos.

Questões internas e externas relevantes que podem ser identificadas incluem:

Questões internas:

- **Ataques de Ransomware**:

  Os ataques de Ransomware são uma ameaça crescente para as empresas de cobrança de dívidas bancárias. Os Ransomware são programas maliciosos que criptografam os dados da vítima e exigem um pagamento de resgate para desbloqueá-los.

- **Incidentes de segurança de funcionários**:
  Os incidentes de segurança de funcionários são uma das principais causas de violações de dados. Os funcionários podem ser vítimas de ataques de phishing ou malware, ou podem cometer erros que levam à exposição de dados confidenciais.

- **Falhas de hardware e software**:
  As falhas de hardware e software podem causar a perda ou corrupção de dados.

Questões externas:

- **Regulamentação**:
  A Bellinati Perez está sujeita a uma variedade de regulamentos de segurança da informação. O não cumprimento desses regulamentos pode resultar em multas ou sanções.

- **Competição**:
  A competição no setor recuperação de ativos. As empresas que não são capazes de proteger seus dados confidenciais podem perder clientes e receita.

Ao identificar e avaliar essas questões, a **Bellinati Perez** desenvolve um SGSI e SGPI eficazes que reduzem o risco de perda de dados, roubo de identidade e outros incidentes de segurança.

A **Bellinati Perez** determina as questões internas e externas, que são relevantes para o propósito da organização e que afetam a sua capacidade de alcançar os resultados pretendidos do SGSI e SGPI, da seguinte forma:

- **Os objetivos da organização**:
  Os objetivos da organização devem ser o ponto de partida para a análise de riscos. Os riscos que podem afetar a capacidade da organização de alcançar seus objetivos devem ser considerados como os mais críticos.

- **O ambiente de negócios**:
  O ambiente de negócio da organização deve ser considerado ao identificar riscos. As mudanças no ambiente de negócios, como a adoção de novas tecnologias ou o aumento da concorrência, podem criar novos riscos.

- **As capacidades da organização**:
  As capacidades da organização devem ser consideradas ao avaliar os riscos. Os riscos que a organização não está preparada para mitigar devem ser considerados como os mais críticos.

ESCOPOS da BELLINATI PEREZ

O escopo de SGSI e SGPI determinado para a **Bellinati Perez** inclui os seguintes aspectos:

- **Limites de aplicabilidade** das normas ISSO 27001 e 27701 no contexto de prestadores de serviços e controladores de dados pessoais dos colaboradores e clientes dos clientes.

- **Ativos de informação**:
  Os ativos de informação da **Bellinati Perez**, são principalmente os dados que trata, sendo o cumprimento das obrigações legais impostas pela lei, na qual inclui o tratamento de dados pessoais e dados pessoais sensíveis de forma segura e transparente.

- **Ameaças e vulnerabilidades**:
  As ameaças e vulnerabilidades que podem afetar os ativos de informação da empresa.

- **Controles de segurança**:
  Os controles de segurança implementados para mitigar os riscos identificados.

- **Processos de segurança**:
  Os processos de segurança implementados para gerenciar a segurança da informação.

Ao determinar o escopo de SGSI e SGPI, a **Bellinati Perez** considera as seguintes questões internas e externas:

Questões internas:

- **Objetivos da empresa**:
  Os objetivos da empresa é o ponto de partida para a determinação do escopo de SGSI e SGPI. Os controles de segurança devem ser implementados para proteger os ativos de informação que são essenciais para a realização dos objetivos da empresa.

- **Ambiente de negócios**:
  O ambiente de negócios da empresa é considerado ao determinar o escopo de SGSI e SGPI. As mudanças no ambiente de negócios, como a adoção de novas tecnologias ou o aumento da concorrência, podem criar novos riscos que devem ser considerados.

- **Capacidades da empresa**:
  As capacidades da empresa são consideradas ao determinar o escopo de SGSI e SGPI. Os controles de segurança devem ser implementáveis e sustentáveis dentro das capacidades da empresa.

Questões externas:

- **Regulamentação**:
  A empresa deve estar em conformidade com os regulamentos de segurança da informação aplicáveis.

- **Políticas e diretrizes**:
  A empresa deve considerar suas políticas e diretrizes internas ao determinar o escopo de SGSI e SGPI.

- **Requisitos das partes interessada**s:
  A empresa deve considerar os requisitos das partes interessadas, como clientes, parceiros e funcionários.

Ao considerar essas questões, a **Bellinati Perez** garante que o escopo de SGSI e SGPI seja adequado para proteger seus ativos de informação e alcançar seus objetivos.

Além das questões internas e externas, o escopo de SGSI e SGPI considera ainda os requisitos das **partes interessadas relevantes**. As partes interessadas relevantes que incluem: **clientes, parceiros, funcionários, acionistas e reguladores**.

Ao considerar os requisitos das partes interessadas, a **Bellinati Perez** garante que SGSI e SGPI atendam às necessidades de todos os stakeholders.

Como a **Bellinati Perez** determina o escopo de SGSI e SGPI:

- **Realiza análise de riscos**:
  A análise de riscos é uma ferramenta essencial para determinar o escopo de SGSI e SGPI. A análise de riscos ajuda a identificar os ativos de informação que são mais críticos para a empresa e as ameaças e vulnerabilidades que podem afetá-los.

- **Conversa com as partes interessadas**:
  As partes interessadas podem fornecer insights valiosos sobre os riscos e requisitos que devem ser considerados ao determinar o escopo de SGSI e SGPI.

- **Documenta o escopo**:
  O escopo de SGSI e SGPI é documentado para garantir que todos os stakeholders tenham uma compreensão clara do que está incluído.

Esta Política de Segurança da Informação poderá ser atualizada em decorrência de eventual atualização normativa.

2. APLICAÇÃO

Esta política se aplica a todos os colaboradores da Bellinati Perez, demais empresas administradas pelo grupo, parceiros, prestadores de serviços e visitantes.

3. CRITÉRIOS E DIRETRIZES

A informação é um importante ativo para a operação das atividades comerciais e para manter a vantagem competitiva no mercado. Tal como os demais ativos da Bellinati Perez, a informação deve ser adequadamente manuseada e protegida.

A atuação da organização inclui a identificação de controles adequados, estruturas organizacionais, desenvolvimento e auditoria de políticas, normas, procedimentos de Segurança da Informação. As violações de política, normas e procedimentos estão sujeitas às sanções disciplinares previstas em normas específicas e legislação vigente.

É imprescindível que todos os funcionários, estagiários e demais parceiros compreendam o papel da Segurança da Informação em suas atividades diárias.

A área de Segurança da Informação administra as disciplinas de conhecimento que dão suporte a essa ciência. A direção e as lideranças devem reconhecer através deste documento que as informações desenvolvidas, operacionalizadas e/ou custodiadas internamente possuem valor intangível e significativo. Dessa forma, se comprometem em garantir os meios necessários para a proteção da informação sob sua guarda, de acordo com os requisitos do negócio e as leis vigentes, bem como devem requerer dos colaboradores e partes externas que pratiquem a Segurança da Informação de acordo com o estabelecido nas políticas e procedimentos. Esta política é o documento oficial que formaliza as orientações sobre Segurança da Informação, devendo ser integralmente observada e cumprida.

O **Comitê Gestor de Crise, de Privacidade de Dados e Segurança da Informação** é formado por representantes gestores das áreas de Cobrança, Jurídico, Administrativo, Financeiro e Tecnologia com a responsabilidade de deliberar sobre assuntos estratégicos da Segurança da Informação, bem como direcionar tomadas de decisão.

É dever do corpo diretivo e lideranças da organização estabelecer os objetivos mensuráveis da Segurança da Informação em relação aos serviços prestados e monitorá-los, garantindo assim a confidencialidade, integridade e disponibilidade da informação, conforme escopo do negócio. Deve ainda assegurar, no que tange a Segurança da Informação, a satisfação das partes interessadas e a reputação da Bellinati Perez.

3.1. INFORMAÇÕES CONFIDENCIAIS

São consideradas informações confidenciais, para os fins desta política, quaisquer informações das partes consideradas não disponível ao público ou reservadas, dados corporativos, dados de negócios e transações, dados pessoais, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pela Bellinati Perez aos seus colaboradores, parceiros e visitantes, em decorrência da execução do contrato de trabalho ou prestação de serviços no país.

São exemplos de informações confidenciais:

(i) Informações de dados pessoais devem ser protegidas por obrigatoriedade legal, tendo como base a Lei Geral de Proteção de Dados Brasileira Lei nº 13.709/2018, incluindo dados cadastrais (CPF, RG etc.), situação financeira e movimentação bancária;
(ii) Informações sobre produtos e serviços que revelem vantagens competitivas da Bellinati Perez frente ao mercado;
(iii) Todo o material estratégico da Bellinati Perez (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);
(iv) Quaisquer informações da Bellinati Perez, que não devem ser divulgadas ao meio externo antes da publicação pelas áreas competentes;
(v) Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.

O colaborador, representante, prestador de serviço, visitante ou parceiro que receber as informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma, uma vez que qualquer revelação das informações confidenciais deverá estar de acordo com os termos e condições estabelecidos pelas políticas e normas da Bellinati Perez. As informações confidenciais somente poderão ser utilizadas para fins de execução das atividades exercidas pela Bellinati Perez em território nacional.

O colaborador, representante, prestador de serviço, visitante ou parceiro deverá resguardar as informações confidenciais de forma estrita, e jamais poderá revelá-las a não ser para os representantes legais da sua unidade de negócios. A parte que receber as informações será responsável por qualquer não cumprimento desta política porventura cometido pelos seus representantes legais. O colaborador, representante, prestador de serviço, visitante ou parceiro deverá informar prontamente a Bellinati Perez sobre qualquer uso ou revelação indevida da informação ou qualquer outra forma que caracterize o descumprimento desta política.

Excetuam-se da obrigação de manutenção de confidencialidade disposta nesta política:

(i) O atendimento a quaisquer determinações decorrentes de lei ou emanadas do Poder Judiciário ou Legislativo, tribunais arbitrais e de órgãos públicos administrativos;

(ii) A divulgação das informações confidenciais aos representantes legais e diretores da Bellinati Perez (incluindo, mas não se limitando, a advogados, auditores e consultores);

(iii) As informações confidenciais que forem divulgadas após o consentimento por escrito do Comitê Gestor de Segurança da Informação.

As cláusulas de ciência, responsabilidade e confidencialidade quanto à política e diretrizes de Segurança da Informação visam alertar e responsabilizar o colaborador, representante, prestador de serviço, visitante ou parceiro, de que o acesso e o manuseio de informação devem se restringir ao exercício da função ou processo que requer essa informação, sendo proibido o uso para qualquer outro propósito distinto do designado.

São responsáveis pela observância desta política os diretores, colaboradores, representantes, visitantes, prestadores de serviços, parceiros e consultores (incluindo advogados, auditores e consultores externos) das unidades da Bellinati Perez.

4. DIRETRIZES PARA SEGURANÇA DA INFORMAÇÃO

A organização deve zelar pela proteção do negócio contra violações de confidencialidade, integridade e disponibilidade de informações. Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.

As diretrizes de Segurança da Informação descritas nesse capítulo e definidas pelo corpo diretivo e Comitê de Segurança da Informação da Bellinati Perez devem ser observadas por todos os colaboradores.

4.1. ATUALIZAÇÃO DE POLÍTICAS, NORMAS E PROCEDIMENTOS

A área de Segurança da Informação será responsável por manter atualizada a Política Corporativa de Segurança da Informação. As normas e procedimentos serão de responsabilidades dos gestores das áreas da empresa. Todas deverão utilizar um processo de validação, aprovação e publicação.

A revisão de todas as documentações pertinentes aos processos de segurança de informação deverá ser realizada ao menos anualmente.

É de responsabilidade dos gestores revisar as documentações de suas áreas, como também enfatizar a seus colaboradores a importância do conhecimento de toda documentação pertinente aos processos de Segurança da Informação.

4.2. SEGURANÇA EM RECURSOS HUMANOS

Antes da contratação devem ser realizadas confirmações das qualificações dos candidatos, considerando a ética, regulamentações e leis relevantes.

Todo novo colaborador, funcionário ou terceirizado, que venha a ter acesso a sistemas e/ou documentos, deve assinar o Termo de Responsabilidade e Confidencialidade de Informações, comprometendo-se assim com o cumprimento da Política Corporativa de Segurança da Informação.

A Bellinati Perez promove a capacitação e qualificação constante aos colaboradores no manuseio das informações, através da disseminação das regras de Segurança da Informação por meio de planos de conscientização contínua, com o objetivo de fortalecer a cultura de Segurança da Informação.

Ao final do contrato de trabalho, o gestor imediato deve imediatamente solicitar a desativação de quaisquer acessos do colaborador e todos os ativos de informática, tais como notebook, celular, tablet, pendrive, quando necessário, ser encaminhado para o departamento administrativo.

4.3. DESENVOLVIMENTO SEGURO

As áreas responsáveis pelo desenvolvimento de sistemas/aplicativos devem incorporar as boas práticas de segurança às atividades de engenharia de software, preservar e salvaguardar os ativos tecnológicos e sistemas sob sua responsabilidade, manter o sigilo sobre as informações de clientes, fornecedores e/ou em sistemas sob sua responsabilidade e contribuir com processo de correção de vulnerabilidades.

4.4. GESTÃO, IDENTIFICAÇÃO E TRATAMENTO DOS RISCOS DE SEGURANÇA

O processo de gerenciamento de riscos possui como objetivo identificar ameaças e vulnerabilidades com potencial de comprometer a Confidencialidade, Integridade e Disponibilidade dos ativos da Bellinati Perez. A execução do processo deve ser periódica garantindo a identificação, classificação, quantificação, qualificação e resposta a todos os riscos mapeados.

Todos os riscos identificados devem ser registrados e acompanhados através de sistemática que armazene todas as informações relevantes para a análise e o tratamento dos riscos.

O processo de gerenciamento de riscos também deve ser realizado em projetos, mudanças e aquisições de tecnologia com o propósito de recomendar controles de segurança necessários, enquanto as análises regulares de vulnerabilidades sobre os ativos de informação devem ser realizadas a fim de identificar e promover o tratamento dos riscos de segurança.

4.5. TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Constitui incidente de Segurança da Informação qualquer ato que viole a confidencialidade, a integridade ou a disponibilidade dos ativos de informação, bem como qualquer acesso indevido aos sistemas ou à infraestrutura de tecnologia pertencentes à Bellinati Perez.

Toda notificação de incidentes de Segurança da Informação ou de uma violação das regras da Política Corporativa de Segurança da Informação deve ser tratada e investigada pela área de Segurança da Informação.

A área de Segurança da Informação deve conduzir o tratamento de incidentes de segurança, avaliar o risco, registrar as ações para remediação com os responsáveis e atuar em conjunto com outras áreas para a resolução do incidente, com transparência, imparcialidade, ética e sigilo.

Após o encerramento do incidente de segurança, a área de Segurança da Informação, caso necessário, deve reportar o caso ao Comitê Gestor de Segurança da Informação. O comité deverá avaliar, e se aplicável, comunicar à diretoria responsável e/ou às áreas de RH e Jurídico que poderão definir sanções disciplinares aos envolvidos no incidente ou acionar autoridades legais.

As violações de segurança devem ser informadas imediatamente ao e-mail ***seguranca@bellinatiperez.com.br***. Toda violação ou desvio devem ser investigados para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

São exemplos de violações de segurança que podem ocasionar sanções:

(i) uso ilegal de software;
(ii) introdução (intencional ou não) de vírus de informática;
(iii) tentativas de acesso não autorizado a dados e sistemas;
(iv) compartilhamento de informações sensíveis ao negócio;
(v) divulgação de informações de clientes e das operações contratadas.

4.6. CONFORMIDADE E MONITORAMENTO

As tecnologias, metodologias, marcas e quaisquer informações que pertençam à estratégia de negócios da organização constituem propriedade intelectual e não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio colaborador em seu ambiente de trabalho. Para manter a conformidade, a Bellinati Perez estimula a cultura de Segurança da Informação como responsabilidade de todos e seguir as normativas, requisitos legais e regulamentares relacionados à Segurança da Informação, conforme:

(i) Todo sistema, sempre que possível, deve gerar trilhas de auditoria que devem ser mantidas para análise posterior e apuração de responsabilidades;
(ii) Todas as trilhas de auditoria devem ser armazenadas e protegidas de acordo com o período exigido por requisitos regulatórios ou contratuais;
(iii) As informações de identificação pessoal dos clientes, dos colaboradores e parceiros devem ser protegidas contra acessos não autorizados, utilizada de forma transparente e apenas para a finalidade para a qual foi coletada;
(iv) Todo ativo é passível de monitoramento e auditoria com a finalidade de cumprir as regras de Segurança da Informação;
(v) As análises críticas e auditorias internas serão realizadas periodicamente de forma a garantir o cumprimento de requisitos de Segurança da Informação externos (Leis e Regulamentações) e internos (Políticas, Normas, Procedimentos e Regulamentos);
(vi) A melhoria contínua dos processos deve estabelecida através das melhores práticas de Segurança da Informação;
(vii) Métricas e indicadores de acompanhamento da efetividade dos processos e controles de segurança da informação devem ser monitorados de acordo com periodicidade estabelecida.

4.7. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações devem respeitar os níveis de sigilo durante sua geração, guarda, uso, transferência e destruição, devendo ser classificada em um dos seguintes níveis:

- **Nível 1: Confidencial** - Documentos que são de acesso a pessoas nomeadas no próprio documento, em uma tabela que contenha os dados de nome, cargo, departamento e empresa, das pessoas que podem acessar o documento.
- **Nível 2: Privado** - Documentos que são para uso da corporação, estes documentos não têm permissão de acesso para pessoas ou empresas que não tem vínculo corporativo ou trabalhista com a Bellinati Perez.
- **Nível 3: Público** - Qualquer documento ao qual tem sua utilização não controlada e o qual não contém informações confidenciais e sensíveis ao negócio.
- **Nível 4: Restrito** – Documento cujo teor não deve ser do conhecimento do público em geral, sendo acessados apenas pelos interessados e por agentes determinados nas quais são tramitados.

4.8. CONTINUIDADE DO NEGÓCIO

Os ativos da Bellinati Perez devem ser avaliados em termos do impacto operacional e do prejuízo financeiro decorrentes de uma eventual paralisação deles.

Os recursos de tecnologia da informação que suportam processos mapeados como críticos devem ser implantados com redundância suficiente para garantir disponibilidade em caso de um incidente grave.

Os planos de contingência operacional devem incluir critérios de acionamento e de retorno, plano de comunicação, plano de escalação, procedimentos operacionais de contingência e um plano de testes regulares para garantir a eficácia dos procedimentos de operação em estado de contingência.

4.9. PROCESSO DISCIPLINAR

Os princípios de segurança estabelecidos na presente política possuem total aderência à administração da Bellinati Perez e devem ser observados por todos na execução de suas funções.

As regras que estabelecem o controle e tratamento de situação de não conformidade ou de exceção relativas a esta Política, Normas ou Procedimentos devem ser descritas em política, procedimento ou norma específica.

Todos os demais casos são considerados uma violação e resultará em medidas disciplinares cabíveis através de sanções administrativas sob a responsabilidade do Departamento de Recursos Humanos da Bellinati Perez, que poderão culminar com o desligamento e eventual processo criminal se aplicável.

5. DIRETRIZES PARA SUPORTE À TECNOLOGIA

5.1. USO DE DISPOSITIVOS MÓVEIS

O colaborador deve zelar pela proteção do dispositivo móvel e das informações nele contidas, seguir rigorosamente a **Política Corporativa de Dispositivos Eletrônicos Móveis**, e ainda:

- Não armazenar informações em dispositivos móveis (pen-drives, hard-drives, memory cards inclusive de telefones e/ou máquinas fotográficas etc.) não autorizados previamente;
- Em locais públicos deve-se manter o dispositivo sempre próximo e à vista, para evitar furtos;
- Em viagem, o dispositivo não deve ser colocado em carrinhos de bagagem dos aeroportos e nem despachado junto com a bagagem.
- Em hotéis o dispositivo deve ser armazenado no cofre do quarto quando disponível;
- Em caso de perda, roubo ou furto, deve-se notificar a área Segurança da Informação através do e-mail seguranca@bellinatiperez.com.br.

5.2. PROTEÇÃO DAS INFORMAÇÕES DURANTE TRABALHO REMOTO

Os cuidados para o trabalho remoto devem ser redobrados, pois a rede do escritório proporciona aos ativos muito mais segurança do que a rede doméstica. Assim, os ativos utilizados em trabalho remoto devem ser protegidos minimamente pelos recursos de VPN, antivírus, possuir os mecanismos de atualização de sistemas e o local de trabalho deve garantir a confidencialidade das informações, apresentadas em tela ou falada.

A Bellinati Perez se compromete a manter e intensificar a conscientização a respeito da segurança da informação aos seus colaboradores, através de campanhas e treinamentos.

5.3. ACESSOS LÓGICOS E FÍSICOS

Cada colaborador ou prestador de serviços deve possuir uma única conta (username /login) pessoal e intransferível, conforme o perfil de acesso definido, devendo os usuários ser identificados e registrados nos acessos aos recursos tecnológicos. Para elevar o nível de segurança dos acessos, os usuários devem definir para si senhas fortes como meio de validação de sua identidade quando dos acessos a estações de trabalho, redes, sistemas, servidores. Toda concessão de acesso lógico deve ser efetuada de acordo com as necessidades de negócio, devendo ser previamente aprovada pelo gestor responsável.

O período de duração da concessão do acesso deve ser pertinente à função do usuário, devendo ser cancelada pelo gestor responsável ao fim do contrato de prestadores de serviço e terceiros ou do desligamento do colaborador.

Periodicamente, as contas dos usuários e seus privilégios nos aplicativos devem ser verificados ou atestados, de forma a promover a manutenção e atualização da base de cadastro, exclusão de usuários desligados, contas em desuso ou em duplicidade e todo acesso físico as dependências da Bellinati Perez devem ser restritas, controlados e monitorados através de mecanismos de controle de acesso e o uso de crachá é obrigatório.

5.4. SEGURANÇA PARA ESTAÇÕES DE TRABALHO

A segurança referente às estações de trabalho possui responsabilidade significativa dos colaboradores e terceiros. Assim, é fundamental seguir as seguintes orientações:

(i) Quando se ausentar da mesa, o usuário deverá bloquear a estação de trabalho, seja notebook ou desktop;
(ii) Sempre que possível, o notebook deve estar preso à mesa com trava;
(iii) A prática de mesa limpa deverá ser adotada, de forma a promover a segurança dos ativos de informação, classificados como confidenciais, bem como o processamento e a guarda de dados críticos devem ser efetuados em áreas com segurança apropriada;
(iv) Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou quaisquer dispositivos, eletrônicos ou não;
(v) Nenhum dado pessoal deve ser deixado à vista, seja em papel ou quaisquer dispositivos, eletrônicos ou não;
(vi) Ao utilizar uma impressora coletiva, recolher o documento impresso imediatamente;
(vii) Não deve ser concedida ao usuário final a permissão de administrador local em sua estação de trabalho;
(viii) Nas estações de trabalho só podem ser instalados softwares devidamente licenciados à Bellinati Perez.

5.5. CONTROLES CRIPTOGRÁFICOS

Os mecanismos específicos de criptografia devem ser adotados para a transmissão e armazenamento de informações classificadas como confidencial, independente do meio de comunicação ou da mídia utilizada para tal.

5.6. CÓPIAS DE SEGURANÇA DOS DADOS (BACKUP)

Considera-se backup qualquer cópia de segurança, quer seja feita em outro dispositivo, como HDs externos, pendrives ou em nuvem. A finalidade do deste procedimento é a pronta recuperação de dados para restaurar informações em caso de perda dos arquivos originais ou em caso de acidentes operacionais com os equipamentos.

Devem ser geradas periodicamente, cópias de segurança dos dados e informações armazenados em servidores, com retenção de acordo a regulação aplicável, respeitando-se a necessidade do negócio. Os dados e informações classificados como restritos e confidencial devem ter atenção especial ao gerar os backups, devendo as fitas ou mídias de armazenagem ter a mesma classificação.

As mídias contendo cópias de segurança devem ser guardadas em um local seguro, com controle de acesso físico, para garantir a disponibilidade, integridade e confidencialidade dos dados de backup caso seja necessário efetuar sua recuperação. Devem ser efetuados testes periódicos de recuperação dos dados, por amostragem, para minimizar o risco de perda de dados por falha de armazenamento.

5.7. DIREITO DE ACESSO (AUTORIZAÇÃO)

O colaborador, parceiro, prestador de serviços é o responsável pela utilização e eventuais usos inadequados dos direitos de acesso que são atribuídos aos seus funcionários, estagiários, prestadores de serviços, parceiros e visitantes, sendo intransferíveis. A solicitação de acesso à informação deve decorrer da necessidade funcional do colaborador, parceiro e prestador de serviços.

5.8. DIREITO DE COLETA E REGISTROS DE ATIVIDADES DE REDE (AUDITORIA)

O colaborador, parceiro, prestador de serviços é o responsável pelas atividades e ações executadas no ambiente de rede da Bellinati Perez e seus respectivos sistemas internos, pois estes devem ser utilizados estritamente para uso corporativo e de negócios do interesse da Bellinati Perez. Desta forma a Bellinati Perez se reserva a coleta, registro, armazenamento e análise de todas as ações executadas e documentos elaborados utilizando-se de equipamentos e dispositivos corporativos e/ou por colaboradores da organização.

5.9. DIREITOS DE PROPRIEDADE

Todo produto resultante do trabalho dos colaboradores, parceiros, consultores e prestadores de serviços (coleta de dados e documentos, sistemas, metodologias, processos, dentre outros) é propriedade da Bellinati Perez. Em caso de extinção ou rescisão do contrato de trabalho ou de prestação de serviços no país, por qualquer motivo, deverá o colaborador, parceiro, prestador de serviços entregar/devolver todas as informações confidenciais geradas e manuseadas em decorrência da prestação dos serviços à Bellinati Perez, ou emitir declaração de que as destruiu.

5.10. EQUIPAMENTOS PARTICULARES/PRIVADOS

Os equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes da Bellinati Perez. Casos de exceção devem ser tratados e autorizados pela área de Segurança de Informação e pela gestão direta do departamento, e seguirem as normas da **Política de Uso dos Dispositivos Eletrônicos Móveis da Bellinati Perez**.

5.11. CONVERSAS EM LOCAIS PÚBLICOS E REGISTRO DE INFORMAÇÕES

É estritamente proibido discutir ou comentar assuntos confidenciais em locais públicos ou por meio de mensagens de texto, exceto quando encaminhadas à Bellinati Perez e direcionada aos interessados.

5.12. NORMAS DE UTILIZAÇÃO DE INTERNET

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a Bellinati Perez, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela, de forma a garantir a integridade de dados e programas. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede.

Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

O uso do correio eletrônico de domínio Bellinati Perez é designado exclusivamente para fins corporativos e relacionados às atividades do colaborador na instituição. A utilização desse serviço para fins pessoais não é permitida.

É proibido:

(i) Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
(ii) Enviar mensagens por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
(iii) Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Bellinati Perez ou suas unidades vulneráveis a ações civis ou criminais;
(iv) Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
(v) Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
(vi) Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da Bellinati Perez estiver sujeita a algum tipo de investigação;

6. RESPONSABILIDADES

A **Diretoria e Gerência** é responsável por:

- Apoiar as diretrizes e princípios de segurança da informação;
- Definir responsabilidades de segurança da informação na Bellinati Perez;
- Fornecer os recursos necessários para as ações de segurança da informação.

A **Segurança da informação** é responsável por:

- Disponibilizar, manter e monitorar os recursos tecnológicos que apoiam as Diretrizes de Segurança da Informação;
- Fornecer suporte e orientação, referente à segurança da informação, para as demais Diretorias e Departamentos da Bellinati Perez;

- Auxiliar na disseminação e conscientização sobre segurança da informação;
- Contribuir para a manutenção da segurança da informação na empresa, ativos tecnológicos e sistemas sob sua responsabilidade;
- Acompanhar e avaliar os projetos de segurança da informação;
- Adequar os serviços, sistemas e ativos de TI de acordo com as recomendações de segurança da informação e as análises de riscos anteriormente realizadas;

Todos os **Colaboradores** são responsáveis por:

- Cumprir sem restrições com esta Política, Normas e Procedimentos de segurança da informação;
- Utilizar apenas as informações previstas pelo seu cargo funcional e por direito de acesso para a realização de suas tarefas;
- Manter o sigilo sobre as informações de clientes, fornecedores e/ou em sistemas sob sua responsabilidade;
- Utilizar de conduta ética no trato com as informações da empresa, clientes e credores;
- Buscar orientação da área de Segurança da Informação em caso de dúvidas relacionadas à segurança da informação;
- Reportar imediatamente à área de Segurança da Informação incidentes de segurança da informação ou violação desta Política e suas Normas e Procedimentos.

7. REVISÃO E ATUALIZAÇÃO

A responsabilidade sobre a revisão, atualização e aprovação prévia das mudanças desta política é do Comitê Gestor de Segurança da Informação. A aprovação final deve ser realizada pela diretoria executiva da Bellinati Perez. A revisão deverá ocorrer em um prazo máximo de 12 meses a partir da aprovação da última versão.

As normas devem ser aprovadas pelo Comitê Gestor de Segurança da Informação e revisadas em um prazo máximo de 12 meses, enquanto os procedimentos devem ser aprovados pelas Diretorias das áreas envolvidas e revisadas em um prazo máximo de 12 meses.

8. DOCUMENTOS RELACIONADOS

- ABNT NBR ISO/IEC 27001:2013: Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão da Segurança da Informação - Requisitos.

9. TERMOS E DEFINIÇÕES

Ativos de Informação - patrimônio composto por todos os dados e informações físicas e/ou digitais geradas, operacionalizadas, armazenadas pela Bellinati Perez.

Informação - É a reunião ou conjunto de dados e conhecimentos resultante do processamento, manipulação e/ou organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano ou máquina) que a recebe.

Gestão de Continuidade de Negócio - é o desenvolvimento preventivo de um conjunto de estratégias e planos para garantir que os serviços, processos e seus recursos essenciais sejam devidamente identificados e recuperados após a ocorrência de eventos adversos, que possam torná-los indisponíveis por um tempo inaceitável.

Gestão de Riscos de Segurança da Informação - processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável.

Risco - combinação da probabilidade da concretização de uma ameaça e suas consequências.

Confidencialidade - garantia de que a informação seja acessada somente por usuários, sistemas ou processos que dispõem de autorização.

Integridade - salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

Disponibilidade - garantia de que os usuários, sistemas ou processos com autorização, obtenham acesso às informações e aos ativos correspondentes sempre que necessário, possibilitando a continuidade do negócio.

Ameaça - causa potencial de um incidente indesejado, que caso se concretize pode resultar em dano.

Vulnerabilidade - fragilidade ou limitação de um ativo que pode ser explorada por uma ou mais ameaças.

Incidente de Segurança da Informação - Evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades e que afete algum dos aspectos da segurança da informação: confidencialidade, integridade ou disponibilidade.

10. CONTROLE DE VERSÕES

Versão	Responsável	Data	Histórico de Atualizações
1.0	Sec2b	22/09/2011	Proposição do documento
1.1	Sec2b	21/10/2011	Atualização de conteúdo
1.2	Sec2b	26/01/2012	Revisão e adequação de termos
1.3	Sec2b	08/03/2012	Revisão e adequação de termos
1.4	Jefferson Limeira	12/11/2012	Revisão, correção de responsabilidades e adequação de termos
1.5	Jefferson Limeira	10/06/2013	Revisão de responsabilidades
1.6	Jefferson Limeira	14/03/2014	Revisão de termos. Adicionado definição de revisão e responsabilidade de normas e procedimentos.
1.7	Jefferson Limeira	03/03/2015	Revisão anual do documento
1.8	Ighor Silva	20/06/2018	Revisão anual do documento
1.9	Helid Bandeira	21/09/2020	Revisão e adequação com a norma ISO 27001
2.0	Jefferson Limeira	10/11/2020	Revisão de termos

3.0	Jefferson Limeira	20/02/2021	Revisão de termos
3.1	Fabio Gomes	03/03/2021	Revisão e adequação à LGPD
4.0	Carlos Moreira	03/03/2022	Revisão geral e anual
5.0	Carlos Moreira	13/06/2023	Revisão de papeis e responsabilidades, segurança dos recursos humanos
6.0	Pio C. F. Jr.	25/09/2023	Revisão dos Propósitos da Organização
6.1	Pio C F Jr	01/12/2023	Revisão de Objetivos e Novas Políticas
6.2	Pio C F Jr	08/12/2023	Revisão e Atualização do Escopo

11. APROVAÇÕES

	Responsáveis	Áreas	Data
VALIDADO POR:	Jefferson Limeira	TI	01/12/2023
VALIDADO POR:	Carlos Moreira	Segurança da Informação	01/12/2023
APROVADO POR:	Luciano Reis	TI	01/12/2023
APROVADO POR:	Pio C. F. Jr.	DPO	01/12/2023

12. CONTROLE DE COMUNICAÇÃO

TIPO DE COMUNICAÇÃO	O QUE COMUNICAR? (Assunto/Tema/ Requisito)	QUANDO COMUNICAR? (Periodicidade)	COM QUEM SE COMUNICAR? (Partes Interessadas)	COMO COMUNICAR? (Meio de Comunicação)	QUEM IRÁ COMUNICAR (Responsável)
Termo de Resp. e Confidencialidade	Relação de termos	A cada 3 meses	Segurança	E-mail, Sharepoint	RH

Planilha de gerenciamento de riscos	Analise de riscos	A cada 3 meses	Segurança	E-mail, Sharepoint	Segurança
Registro do tratamento de incidentes de segurança	Relação de incidentes	Mensalmente	Segurança	E-mail, Sharepoint,	Segurança
Planos de contingência operacional	Relação de planos	A cada 3 meses	Segurança	E-mail	Segurança