Política de Segurança

. Introdução

No site https://nbep.com.br/ nós desenvolvemos soluções bem simples e seguras, 100% digitais no intuito de ter o controle de suas interações totalmente em suas mãos. Nós valoramos as ações de nosso público-fã e de nossos usuários, e demais visitantes, visando atender nosso público alvo, de forma segura e entendemos que a segurança cibernética é de suma importância para que todos possam gozar de nossos Serviços, com qualidade e transparência.

Em nosso site https://nbep.com.br/ praticamos a estratégia de defesa em profundidade ao implementamos camadas diversas de segurança, para mitigar qualquer possível comportamento suspeito de qualquer camada de nossa defesa virtual e digital.

Saiba que, a segurança das suas informações está em nosso DNA e, quando possível, disponibilizaremos aqui um resumo da nossa **Política de Segurança Cibernética** *Política* visando fazer com que você passe a ter um pouco mais de conhecimento sobre as nossas diretrizes quando da proteção de seus dados de acesso.

Escopo

Saiba que, todos os que estão sujeitos as políticas da empresa são aqueles vinculados ao nosso certame, bem como aqueles que, de alguma forma, colaboram para o Bem comum da empresa e do bom

funcionamento de nosso site (https://nbep.com.br/) e neste caso, incluímos os funcionários, os consultores, os terceiros, os fornecedores, os parceiros, bem como os nossos próprios usuários, visitantes e público-fã, caso esses acessem, ou armazenem, ou processem, ou até mesmo transmitam qualquer informação que nos pertença ou sob a guarda de nossa instituição **Negros, Brancos & Pretos Ltda** ou **NB&P Ltda** do site https://nbep.com.br/ .

Objetivo

1. Exigir, registrar e firmar confidencialidade, integridade e disponibilidade de todas as informações que por direitos e guarda pertencem ao certame **Negros, Brancos & Pretos Ltda** e ao site https://nbep.com.br/;
2. Criar e manter medidas que vige proteger a estrutura que suporta os nossos Serviços e nossas atividades de negócio junto ao site https://nbep.com.br/;
3. Atenção na prevenção, ao detectar e ao reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético de nosso site https://nbep.com.br/.

Princípios de Segurança da Informação

Nossa confidencialidade: é garantir que todas as informações que são disponibilizadas e divulgadas, que apenas os indivíduos, as entidades ou processos sejam autorizados a ter acesso e conhecimento junto ao site https://nbep.com.br/;

Nossa integridade: é garantir que as informações sejam precisas, completas e protegidas de quaisquer alterações indevidas, intencionais ou acidentais;

Nossa disponibilidade: é garantir que as informações sejam acessíveis e utilizáveis sob demanda por cada usuário, entidades ou processos autorizados.

Diretrizes

- O acesso ao site (https://nbep.com.br/) e seus sistemas, seus recursos e outros ativos de informação devem ser concedidos mediante a uma autenticação válida – quando houver – e baseado em:

- Grande possibilidade de se fazer negócios conosco;
- Observância do princípio do menor privilegiado; e
- Soluções em relação à segregação de funções;

- Os acessos ao site devem ser gerenciados através de um ciclo de vida desde a entrada até a saída e o seu tempo de permanência, criação até a desativação, incluindo revisões periódicas quanto à precisão e adequação;
- Com relação aos e-mails a composição das senhas deve seguir os requisitos de complexidade e ser únicas. Não devem ser reutilizadas, compartilhadas, armazenadas em arquivos ou escritas em qualquer lugar;
- Observe que Logs e trilhas de auditoria devem ser habilitadas em ambientes de produção, protegidos de acessos e alterações não autorizados e registrar:

- Qual atividade foi executada no site;
- Quem executou qualquer atividade no site;
- Quando a atividade foi executada no site;
- No que consiste a execução de certa atividade no site;

- Os algoritmos criptográficos devem ser aplicados conforme a necessidade em dados em repouso, em trânsito e/ou em uso;
- Criação de ferramentas e processos para monitorar e impedir que informações sensíveis deixem o ambiente interno de uma organização sem autorização devem estar implementados;
- As soluções e/ou processos que permitam a prevenção, detecção, e identificação de ataques à componentes da infraestrutura do site (https://nbep.com.br/) devem estar implementados;
- Acionamos um processo de gerenciamento do ciclo de vida de vulnerabilidades, desde a identificação até a remediação, incluindo diretrizes para documentação, emissão de relatórios e divulgação deve estar implementado em nosso site (https://nbep.com.br/);
- Soluções de software anti-malware de detecção, prevenção e recuperação ou controles equivalentes devem estar implementadas para proteger o ambiente do NB&P LTDA, cabendo aos responsáveis pela hospedagem, o seu pronto reestabelecimento, sem prejuízos de possíveis danos à NB&P;
- Avisos de informação considerados spans ou suspeita de fraude, que armazenem e/ou processem informações sensíveis ou suspeitas, devem ser restringidos às áreas segregadas da rede, com controle de acesso apropriado, cabendo ao provedor de hospedagem e a empresa e ou responsável (is) pela hospedagem, solucionar esses possíveis problemas;
- Bancos de dados de produção devem possuir backups suficientes para restaurar o funcionamento dos sistemas no

evento de uma perda de dados ou interrupção de serviço e essa responsabilidade recai sobre os profissionais e suas empresas de hospedagens do site (https://nbep.com.br/);

- Durante o ciclo de vida de desenvolvimento de nosso site, requisitos de segurança devem ser aplicados para garantir a confidencialidade, integridade e disponibilidade das informações;
- Observe que deve ser feita uma avaliação de segurança antes da implementação de qualquer nova tecnologia, ferramenta ou solução em produção dentro de nosso portal, rede, app ou site;
- Os procedimentos e os controles, esses voltados à prevenção, tratamento, e redução da vulnerabilidade do site (https://nbep.com.br/) a incidentes de segurança cibernética, além das diretrizes para registro, análise de causa e impacto, e avaliação da relevância de incidentes, devem estar implementados junto a empresa **Negros, Brancos & Pretos**.,;
- As informações devem ser classificadas para auxiliar no mapeamento consistente dos usuários e público-fã e estabelecer o nível de proteção adequado em seu armazenamento de dados e de dados de transmissão e de uso de nossos Serviços;
- Nosso Plano de Continuidade de Negócios (PCN) busca garantir que, em situação adversas, os processos essenciais e críticos sejam devidamente mantidos, preservando assim a continuidade de funções de negócios, operações e serviços críticos. O PCN deve ser testado anualmente.
- Sabemos que treinamentos de conscientização devem ser de caráter obrigatórios a se realizar uma vez por ano, e que apresente os princípios básicos de segurança da informação no intuito de auxiliar os colaboradores, usuários e público-fã no reconhecimento de situações de risco para agir corretamente;
- Todo e qualquer consumo, compartilhamento de informações de incidentes bem como ameaças com outras redes ou sites e até

mesmo instituições, que sejam locais, regionais ou globais deve ser feito por canais seguros junto aos nossos Serviços;
- A Política de Segurança Cibernética do **Negros, Brancos & Pretos** deve ser revisada, no mínimo, anualmente.

Recomendações de Segurança para Visitantes Usuários, Colaboradores e Público-fã

- Você deve criar senhas complexas e deve utilizar seus dados ou informações pessoais na seguinte composição (ex.: nomes de familiares ou data de nascimento). Sempre dê destaque para senhas que sejam compostas de pelo menos 5 palavras aleatórias;
- Faça alteração de sua senha sempre que perceber algum indício ou suspeita de vazamento, ou comprometimento das suas credenciais de login;
- Seja prudente, evite utilizar a mesma senha em mais de um serviço, de preferência e se possível use um gerenciador de senhas para o armazenamento e gerenciamento de credenciais de login;
- Saiba que sua senha é pessoal e intransferível, logo não a compartilhe com estranhos e nem faça anotação em lugares que outras pessoas tenham facilidade em acessar (ex.: blocos de notas, cadernos, agendas, etc.,);
- De preferência para habilitar um segundo fator de autenticação (ex.: SMS, biometria ou reconhecimento facial);
- Sempre evite acessar sites e aplicativos suspeitos ou realizar buscas com a janela de nosso site (https://nbep.com.br/) aberto em computadores, celulares e tablets de terceiros, e públicos

(ex.: Lan House) ou não confiáveis. O mesmo vale para redes wireless (Wi-Fi) públicas;

- Para ter um melhor desempenho ao acessar nossos Serviços em nosso site (https://nbep.com.br/) mantenha seus dispositivos com os sistemas operacionais e aplicativos atualizados;
- Sempre procure instalar uma solução de antivírus no seu computador e sempre mantenha atualizada;
- Sempre evite abrir e-mails cujo remetente ou conteúdo sejam desconhecidos, mesmo que possa observar nossa marca;
- Não clique em links disponibilizados em e-mails ou em mensagens SMS suspeitas e/ou desconhecidas, sem ter certeza que são links válidos enviados por nós;
- Nunca realize o download ou execute quaisquer arquivos anexos em quaisquer e-mails que sejam suspeitos (ex.: com tom de urgência ou com erros gramaticais);
- Você nunca deve informar seus dados pessoais, corporativos ou financeiros para nós em ligações, ou mensagens recebidas de pessoas desconhecidas. Se lembre que o mesmo vale para sites suspeitos, spam e sempre verifique se o site que você está acessando é realmente o verdadeiro (https://nbep.com.br/);
- Sempre bloqueie o dispositivo móvel suspeito de ter sido utilizado para acessar sites e aplicativos suspeitos;
- Nunca empreste seu celular para pessoas desconhecidas;
- É importante você manter pelo menos uma cópia de segurança (print) da tela da página do site que visitou.