

Desenvolvimento de Políticas de Segurança





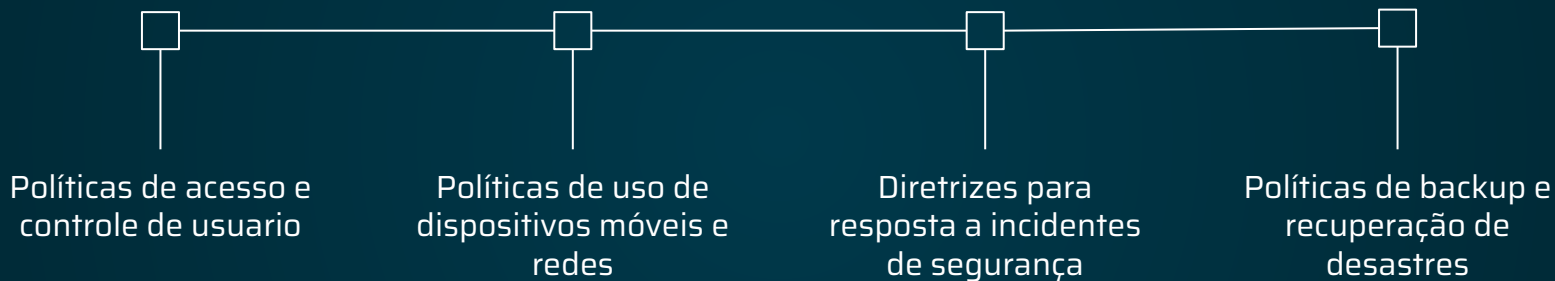
Quem é o nosso
cliente?



Cassino Judas Online

O Cassino Judas precisam diariamente lidar com uma quantidade significativa de dados financeiros e pessoais sensíveis, além de transações monetárias frequentes. Em que precisa garantir o controle de acesso e a proteção das contas de usuários que é crucial para evitar fraudes, roubo de dados e comprometimento do sistema de apostas.

Conjunto de Políticas de Segurança





01

Políticas de Acesso e controle de usuario

Políticas de Acesso e controle de usuário



01 Autenticação de Dois Fatores (2FA)

02 Política de Senhas Fortes

03 Bloqueio de conta por tentativas inválidas

04 Segregação de Privilégios de Acesso

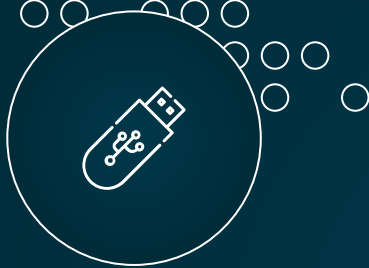
05 Revisão Periódica de Privilégios de Acesso

06 Monitoramento e Registro de Acessos

07 Desconexão Automática por Inatividade

08 Contas Administrativas Dedicadas

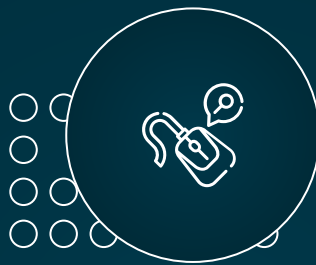
09 Monitoramento de transações e apostas suspeitas



Autenticação de Dois Fatores

Exigindo uma segunda verificação como um código enviado para o celular ou um token.

Justificativa: O 2FA adiciona uma camada extra de segurança, tornando mais difícil para invasores comprometerem uma conta, mesmo que consigam a senha.



Política de Senhas Fortes

8 caracteres, maiúsculas, minúsculas, números e símbolos. Além disso, senhas devem ser trocadas a cada 90 dias.

Justificativa: Senhas fortes dificultam ataques de força bruta ou engenharia social. Trocas regulares ajudam a mitigar o risco de senhas comprometidas.



Bloqueio de conta por tentativas inválidas

A conta é temporariamente bloqueada, após 5 tentativas.

Justificativa: Limitar o número de tentativas reduz a probabilidade de ataques de força bruta bem-sucedidos.



Monitoramento e Registro de Acessos

Sistema que registre todos os acessos e tentativas de acesso, permitindo auditorias e detecção de atividades suspeitas.

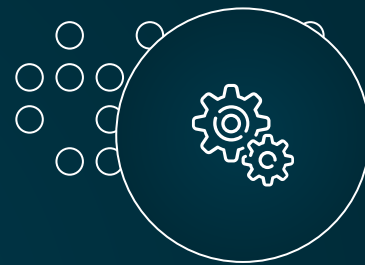
Justificativa: O registro de acessos é crucial para identificar violações de segurança e para cumprir com auditorias de conformidade.



Segregação de Privilégios de Acesso

Dividir os níveis de acesso com base nas necessidades de trabalho dos usuários, só acessar o que é essencial para suas funções.

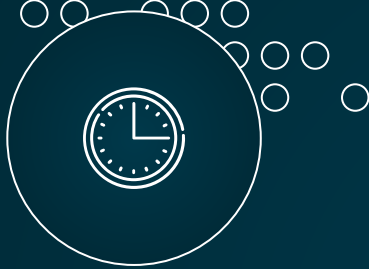
Justificativa: A segregação de privilégios minimiza o impacto potencial em caso de violação, pois limita o que um invasor pode acessar.



Revisão Periódica de Privilégios de Acesso

Auditorias regulares para revisar e ajustar os privilégios de acesso dos funcionários

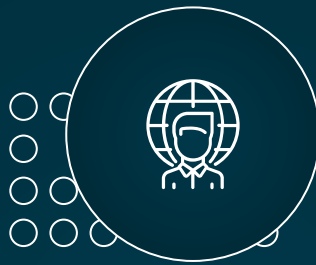
Justificativa: Funções e responsabilidades mudam, e revisar regularmente os acessos evita que usuários mantenham privilégios desnecessários.



Desconexão Automática por Inatividade

Desconexão automática de usuários após um período de inatividade

Justificativa: Desconexões automáticas evitam que estações de trabalho abandonadas permaneçam logadas.



Contas Administrativas Dedicadas

Contas de administrador separadas para tarefas críticas, e garantir que essas contas não sejam usadas para atividades diárias, como navegação na web.

Justificativa: Limitar o uso de contas com altos privilégios, garantindo que elas sejam usadas apenas quando absolutamente necessário.



Monitoramento de Transações e Apostas Suspeita

Monitorar atividades de apostas e transações financeiras detectando padrões de comportamento atípicos

Justificativa: Ajudando a identificar fraudes, lavagem de dinheiro e atividades de manipulação de jogos.

A collection of isometric icons in shades of teal and light blue. The icons include a large shield with a checkmark, a padlock, several cloud shapes, and speech bubbles. The background is dark teal with decorative patterns of white circles and a large teal ring on the left.

02

Políticas de uso de dispositivos móveis e redes

Políticas de uso de dispositivos móveis e redes

01

Segurança de Dados
Pessoais

02

Segurança da Rede

03

Compatibilidade e Atualizações
de Software

04

Uso Responsável

05

Prevenção de Fraudes

06

Privacidade do Usuário

07

Proibições e Restrições

08

Termos de Conectividade





Segurança de Dados

Pessoais

Proteção de dados: O cassino online deve garantir que todos os dados pessoais e financeiros dos usuários sejam criptografados e armazenados de forma segura.

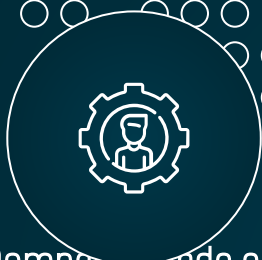
Justificativa: A proteção de dados é crucial, já que os cassinos online lidam com informações sensíveis, como dados pessoais e financeiros.



Segurança da Rede

Acesso a partir de redes públicas: A política deve desencorajar o uso de redes públicas ou não seguras.

Justificativa: Redes públicas e não seguras são vulneráveis a ataques, como interceptação de dados ou tentativas de phishing. Orientar os usuários a evitá-las é uma maneira de minimizar os riscos de fraudes e roubos de informações. Além disso, monitorar o uso de VPNs pode ajudar a evitar abusos, como manipulação de localizações geográficas ou fraude.



Compatibilidade e Atualizações de Software

Dispositivos compatíveis: O cassino deve listar os requisitos mínimos de hardware e sistema operacional.

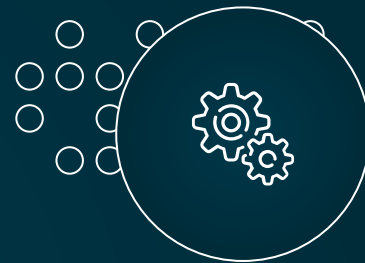
Justificativa: Dispositivos e softwares desatualizados podem ser vulneráveis a malware ou falhas de segurança. Garantir que os usuários estejam cientes dos requisitos mínimos de hardware e que mantenham seus dispositivos atualizados reduz as chances de brechas de segurança.



Uso Responsável

Tempo de uso: O cassino pode recomendar limites de tempo para evitar o uso excessivo

Justificativa: Promover o uso responsável dos dispositivos móveis ajuda a prevenir comportamentos compulsivos ou dependência de jogos de azar. Notificações automáticas e lembretes sobre o tempo de jogo podem ajudar os usuários a manterem-se conscientes.



Prevenção de Fraudes

Monitoramento de comportamentos suspeitos:

Justificativa: A detecção de padrões de comportamento suspeitos é essencial para proteger o cassino e os jogadores de fraudes, como o uso de contas múltiplas ou de bots para manipular resultados.



Privacidade do Usuário

A política deve garantir que dados de dispositivos móveis (como localização, ID do dispositivo ou histórico de navegação) não sejam compartilhados com terceiros sem o consentimento explícito do usuário.

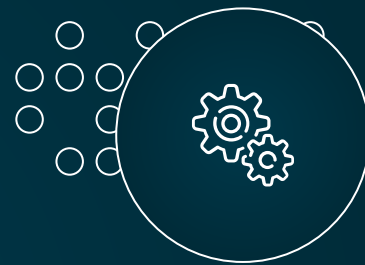
Justificativa: Os jogadores confiam que suas informações pessoais e dados de navegação serão protegidos. Ao garantir que não compartilham esses dados sem consentimento, o cassino respeita a privacidade dos usuários, aumentando sua confiança na plataforma.



Proibições e Restrições

Tempo de uso: O cassino pode recomendar limites de tempo para evitar o uso excessivo de dispositivos móveis durante o jogo, promovendo o jogo responsável.

Justificativa: Bots, scripts ou outras ferramentas de automação podem dar vantagem injusta a alguns jogadores e comprometer a integridade dos jogos.



Termos de Conectividade

Monitoramento de comportamentos suspeitos: O cassino deve detectar padrões atípicos, como acessos repetidos de múltiplos dispositivos ou localizações em curto prazo.

Justificativa: Em jogos online, desconexões involuntárias podem acontecer devido a falhas de rede ou problemas nos dispositivos móveis.

An isometric illustration featuring a central shield with a checkmark, a padlock, and several speech bubbles, all surrounded by stylized cloud shapes. The entire scene is set against a dark teal background with decorative patterns of white circles and a large teal circular shape on the right.

03

Diretrizes para resposta a incidentes de segurança

Diretrizes para resposta a incidentes de segurança

01

Preparação e Planejamento

02

Deteção e Identificação

03

Contenção e Mitigação

04

Erradicação

05

Recuperação

06

Comunicação

07

Análise Pós-Incidente

08

Conformidade e Auditoria





Preparação e Planejamento

Política de Segurança: Define diretrizes claras para responder a incidentes, garantindo que todas as equipes saibam suas responsabilidades.

Equipes de Resposta (CSIRT): Ter uma equipe treinada agiliza a resposta a incidentes, minimizando danos e tempo de recuperação.

Monitoramento Contínuo: Detecta anomalias em tempo real, permitindo ações rápidas contra fraudes e invasões.

Testes Regulares: Simulações periódicas ajudam a identificar vulnerabilidades antes que sejam exploradas.



Detecção e Identificação

Monitoramento de Logs: A análise contínua de logs permite identificar acessos suspeitos e tentativas de intrusão.

Sistemas de Detecção de Intrusões (IDS/IPS): Automatiza a identificação de atividades maliciosas, garantindo alertas em tempo real.

Relatórios de Jogadores: Estimula os usuários a reportarem problemas, complementando o monitoramento técnico.



Contenção e Mitigação

Isolamento de Sistemas Afetados: Limita a propagação do ataque, minimizando seu impacto na organização.

Ativação de Planos de Contingência: Mantém a continuidade dos serviços durante a contenção de ataques, evitando paralisações.

Bloqueio de Contas Suspeitas: Protege o sistema enquanto a investigação está em andamento, evitando fraudes adicionais.

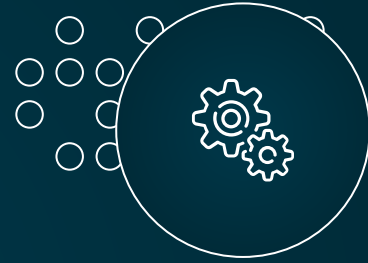


Erradicação

Remoção de Ameaças: Elimina as causas da intrusão, prevenindo novas ocorrências.

Patches e Atualizações: Fecha brechas de segurança, impedindo que sejam reutilizadas em ataques futuros.

Revalidação de Sistemas: Garante que os sistemas estejam seguros antes de serem reintegrados, evitando reincidências.



Recuperação

Restauração de Sistemas: Recupera dados e sistemas comprometidos usando backups, restaurando a operação normal de maneira segura.

Reativação de Contas: Restabelece o acesso dos jogadores após a confirmação de segurança, garantindo que não haja mais riscos.

Monitoramento Aumentado: Aumenta a vigilância nos sistemas restaurados para detectar qualquer atividade residual ou novas tentativas de ataque.



Comunicação

Notificação Interna: Informa todas as partes envolvidas sobre o incidente, garantindo uma resposta coordenada e eficiente.

Comunicação com Reguladores: Assegura conformidade legal e preserva a credibilidade da organização.

Aviso aos Jogadores: Mantém a transparência e orienta os usuários sobre medidas de proteção, reforçando a confiança.



Análise Pós-Incidente

Relatório Completo: Documenta o incidente e as lições aprendidas, melhorando a preparação para incidentes futuros.

Ajustes nas Políticas de Segurança: Ajusta as políticas com base nas vulnerabilidades identificadas, fortalecendo as defesas.

Treinamento Contínuo: Capacita a equipe para lidar com novas ameaças, mantendo-se atualizada sobre as melhores práticas de segurança.



Conformidade e Auditoria

Revisão de Conformidade: Garante que todas as ações sequem as normas e regulamentações, evitando penalidades legais.

Auditorias Regulares: Mantém a eficácia das medidas de segurança e protege os dados dos jogadores, garantindo que as políticas estão sendo aplicadas corretamente.

A collection of isometric icons in shades of teal and light blue. The icons include several cloud shapes, two speech bubbles, a large shield with a checkmark, and a padlock. These icons are arranged in a cluster, suggesting themes of cloud security and data protection.

04

Políticas de backup e recuperação de desastres

Políticas de backup e recuperação de desastres

01

Backup de Dados

02

Políticas de Retenção de
Dados

03

Planos de Recuperação de
Desastres

04

Testes Regulares de Backup
e Recuperação

05

Segurança e Conformidade

06

Mitigação de Ciberataques Avançados

07

Redundância de Infraestrutura

08

Plano de continuidade de negócios(BCP)

09

Proteção contra Erros Humanos





Backup de Dados

Frequência de Backup:
Backup em Tempo Real:
Backup em Múltiplas Localizações:
Criptografia de Backup:

Justificativa: A proteção de dados frequente e distribuída geograficamente evita interrupções prolongadas e vazamentos de dados.



Políticas de Retenção de Dados

Período de Retenção:
Eliminação Segura de Dados.

Justificativa: A retenção e exclusão seguras de dados previnem problemas legais e protegem a privacidade dos jogadores.



Planos de Recuperação de Desastres

Identificação de Riscos:
Recuperação de Sistemas Críticos:
RTO e RPO.

Justificativa: Um plano claro garante que operações essenciais sejam restauradas rapidamente, minimizando interrupções e prejuízos.



Testes Regulares de Backup e Recuperação

Testes de Backup:
Simulações de Desastres:
Auditoria de Conformidade.

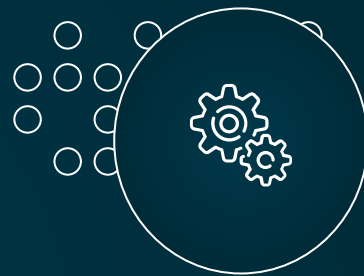
Justificativa: Testar regularmente as soluções evita falhas no momento da necessidade, aumentando a confiança no processo.



Segurança e Conformidade

Conformidade com Regulamentos de Jogo:
Monitoramento Contínuo:
Planos de Comunicação de Emergência.

Justificativa: Conformidade e comunicação clara mantêm a confiança e evitam sanções legais.



Mitigação de Ciberataques Avançados

Recuperação de Ransomware:
Segurança de Rede.

Justificativa: A proteção contra ataques cibernéticos reduz o impacto de ransomwares e mantém a integridade da infraestrutura.



Redundância de Infraestrutura

Infraestrutura de Alta Disponibilidade: Balanceamento de Carga.

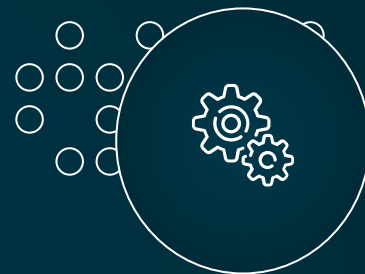
Justificativa: Reduz o tempo de inatividade e mantém a experiência dos jogadores durante falhas ou desastres.



Plano de continuidade de negócios(BCP)

Apoio Operacional Alternativo: Responsabilidades e Treinamento.


Justificativa: Um BCP eficaz mantém as operações e a equipe pronta para responder a qualquer emergência.



Proteção contra Erros Humanos

Controle de Acessos: Versionamento de Backup.

Justificativa: Previne a perda de dados por erro humano, garantindo controle e recuperação de informações.

An isometric illustration on a dark teal background featuring several icons: a laptop, a cloud, a speech bubble, a shield with a checkmark, a smartphone, and a padlock. These icons are interconnected by white lines, suggesting a network or system. The background is decorated with a grid of small white circles and a large white circle in the upper left.

Obrigado pela atenção!

Matheus Yusuke Minakawa - 82416000

Matheus Henrique - 82410661

Gustavo Amorim - 824134456

Gabriel Pessini - 824129852

João Gobbi - 824145710

Matheus Santos - 824212452

