TERMOS DE RECURSOS DE ABUSE

Curitiba, 15/01/2019 – CNPJ 20.962.496/0001-91 – IDC 2112 – REG: 05/06/2014
Registro Contrato e termos de uso de dados e exclusividade

1. PROCESSOS DE ABERTURAS:

Como atuamos com as denúncias de abuso.

1. Nossa equipe averiguará a denúncia e determinar a categoria do abuso.
2. No caso de domínio hackeado/prejudicado, um aviso será enviado para o domínio denunciado. Caso o denunciado se recuse a retirar o conteúdo não autorizado, o domínio será suspenso.
3. No caso de abuso deliberado como: fraude, Malware, scan, pornografia infantil, o domínio será suspendido de imediato por espécie qualquer não reembolsável.
4. No caso de violação de dados, senhas, e-mails e painéis violados, credenciais, acessos serão negados.

2. SOBRE A SEGURANÇA HOSTING

Todas as diretrizes são atendidas em nosso sistema Hosting para qualquer processo seguro a qual o cliente tem por meio de uma única conta, a conexão total de seu servidor Hosting seguindo os critérios de segurança e CPI Security. Em base de uma criação de conta com um e-mail devidamente validado, este é total responsável para a utilização de acesso e controle total de suas atividades para qualquer aspecto sobre a provedora desde o acesso legítimo e as ações como: Alerta de Login, Notas de atualizações, Boletos para pagamentos, Alertas de instabilidades, Recursos de implantação e qualquer outra tratativa que este e-mails é devidamente autorizado.

3. ATIVIDADES DO CLIENTE

Todo qualquer acesso vindo da conta cadastrada como: acesso no painel, boletos pagos e qualquer atividade de cota é devidamente autenticada e gerada o controle de logs, a qual o cliente pode saber exatamente as ações.

1. Alteração de Dados perfil
2. Alteração de Senha
3. Login com Sucesso na conta
4. Falha de login na conta
5. Boletos pagos e gerados
6. Controle de Chamados tickets
7. IP coletado em cPanel
8. Logs de atividades cPanel Este meio de tecnologia possibilita o cliente a unificação de dados e procedimentos seguros uma vez que apenas este e-mail cadastrado é autorizado a delegar as ações informadas e podem atuar em conformidade com o painel.

4. SEGURANÇA DA CONTA

O Painel é munido de camadas de segurança adicionais para proteção do cliente evitando que este seja invadido uma vez que o uso de e-mails gratuitos pode quebrar totalmente as camadas, já que não temos o controle dos servidores gratuitos como:
@Gmail, @Yahoo, @Hotmail entre outros. Portanto é preciso que o cliente seja ciente que usar contas gratuitas e não seguir os critérios de segurança para esta conta desde ativação de 2F fatores de segurança, ativação de PIN, ativação de contas resgates, ativação de celulares para autorização podem comprometer os dados, estes levados para este e-mails de cadastro. As ações das camadas atuam e conformidades com protocolos

Nacionais e Internacionais e podem diretamente atuar com as seguintes normas de segurança:
1. O cliente errar o e-mail ou senha por 3x (três vezes) é acionado o alerta login / Falha de login
2. O cliente errar o e-mail ou senha por 4x (quatro vezes) é ativado o PIN / Pino de segurança
3. O cliente com o PINO ativo, é necessário informar o número do pino no e-mail de cadastro.
4. O cliente não informar o pino de segurança sua conta manterá bloqueada até que este informe
5. O cliente ao solicitar apoio técnico via chat, terá que informar o TOKEN de segurança em sua conta
6. Se todas as informações não forem atendidas, o cliente pode sofrer penalizações e suspensão de conta.
7. Nenhuma conta cPanel é fornecida para o cliente, o Painel possui autoridade ID API autoconecte.

5. SOBRE A CAMADA DE PROTEÇÃO PIN

O que é o PIN código de Secreto? O login de segurança adicional uma camada adicional para sua conta. Se o usuário falhar no login, tentar 03x vezes ou mais, o usuário lembra sua senha e efetua o login com sucesso.

Ele precisa digitar uma segunda senha que será enviada para o e-mail dele, para garantir que o usuário é ele, e ele é quem está tentando fazer login com sua conta cadastrada e-mail verificado. Conta e não é outro usuário, abuso ou boot tentando obter a conta do usuário.

Por que você precisa disso? Senha muitos fracas podem ser adivinhados. Portanto, o login de segurança oferece segurança adicional para parar de adivinhar a senha x vezes, por exemplo, definimos o login de segurança para três ou mais tentativas de login com falha e o usuário tentar fazer login na área do cliente duas vezes e falhar.

Na área do cliente, o login de segurança impedirá que o usuário acesse sua conta e lhe envie um código secreto, se ele digitar corretamente o código, ele será redirecionado para a área do cliente e logs são coletados como IP do equipamento, Rede virtual Privada VPN, ASN e ISP local etc.

Característica:

A proteção é ativada quando alguém faz login em sua conta incorretamente ou por 3 tentativas com erros ou mais. Alguém tentando fazer o login utilizando seu e-mail de cadastro ou adivinhações que não possa ter o acesso.

Desativa sua conta temporariamente se ocorrer mais falhas e enviar um e-mail novamente com o código para o acesso. Desativa a conta, se ocorrerem falhas suficientes, até que o proprietário da conta envie o código secreto para desbloquear a conta.

O cliente deve informar o código secreto de acesso em sua conta a qualquer momento para conectar-se corretamente. Forçar todos os usuários cadastrados em seu painel como subcontas a informar o código para conexão de contas se solicitados. Somente o e-mail

cadastrado do cliente pode ver seu código secreto recebendo um código de recuperação no e-mail. Saiba mais em: https://www.hostcuritiba.net.br/painel/pin.php

Nota: Se o cliente tem o acesso a conta, as ações foram devidas aos e-mails de cadastro ser acessível, hackeadas ou disponível publicamente sem qualquer segurança a qual apenas estes e-mails possuem dados sensíveis do Hosting, e portanto é imprescindível que se use e-mails do próprio domínio, não usar contas gratuitas se estas não seguras. Senhas como cPanel não são fornecidas no servidor por já possuir ID Conecte, auto conecta-se via nosso painel de controle, tornando mais seguro seu acesso devido as camadas que este possui e bloqueando qualquer tentativa de senha manual usada para autenticar acesso cPanel este com auto login apenas via nosso painel de controle e logs monitorados gerados em conformidade com a segurança das camadas. Senhas cPanel devem ser solicitadas via ticket.

6. SOBRE A CAMADA DE PROTEÇÃO TOKEN

O que é Token e porque preciso disso? O Token do cliente é usado para verificar se você é o titular legítimo da conta e não alguém tentando se passar por você ao usar nosso suporte via chat, e-mails ou telefones.

O seu Token de Suporte será válido por 12 horas a partir do momento em que você gerar e só poderá ser usado podendo alterar aleatoriamente de acordo como mês e devidamente circular de códigos alternando a cada mês pelo sistema automatizado e as atividades consideradas como alerta de atenção por uso, de senhas erradas, redes de acessos por Rede virtual privada (Virtual Private Network) VPN.

Quando um cliente registra-se e recebe seus dados completos como: Número do Pedido, Token de acesso, Número do Contrato e suas credenciais, é gerado um bloco de IP local a qual sempre que este acessado e controlado pelas ferramentas de monitoramento no NOC, podem exigir que o operador solicite o Token se uma rede externas for solicitada como uso de VPN, Roteadores, Acessos exterior ou falsa informação, considerando que o retorno de atendimento é controlado e o operador é devidamente treinado e observado em suas ações frequentes para a identificação de fraude. Saiba mais em: https://www.hostcuritiba.net.br/painel/index.php?m=supportpin

SOBRE A CAMADA (2F) DOIS FATORES

O que é Dois fatores 2F e porque devo ativá-lo? A pergunta de segurança ajuda a proteger a sua conta de redefinições de senha não autorizadas e nos permite verificar a sua identidade quando solicitando conta as mudanças.

O cliente ao cadastrar uma pergunta de Segurança, esta não é enviada para o e-mail legitimando o cliente de alegações de alterações de dados a qual somente o cliente humano é possível saber sobre a criação de sua resposta secreta a qual mesmo que sua conta fora invadida, a pergunta não será aceita se estiver errada e sua senha não será alterada com a função ativa.

A Segurança de Camada 2F possibilita que mesmo que o usuário acesse seu painel, não alterar dados, não alterar senha e isso e sua atividade e tentativas homologadas e controladas pelo gerador de logs do seu Painel que podem ser visto com as atividades recentes.

Nota: Se o usuário conseguiu alterar dados, senhas e gerou as suas atividades mesmo que este use redes anônimas, roteamento de redes, Redes Virtuais Privadas VPN ou qualquer outra ferramenta de ofuscação de redes, sabemos que isso é visível e ninguém pode se esconder em redes fora de TOR/P2P.

Portanto é legítimo que o usuário do acesso a qual tenha feito a alteração, munia de todas as credenciais de acesso ou possui certamente a porta de entrada das informações que são a sua conta de e-mail cadastrada.

Seguir regras de segurança 2F e para senhas fortes, e seguras seriam suficientes para evitar isso.

Sobre a segurança de contas Google:
https://support.google.com/accounts/answer/185839?co=GENIE.Platform%3DDesktop&hl=pt-BR

Nossos termos de uso e Responsabilidades você deve saber em:
https://www.hostcuritiba.net.br/painel/termos.php

PROCEDIMENTOS DE RECUPERAÇÃO
Como eu devo proceder para recuperar meus dados? De acordo o as nossas políticas de dados, segurança e seguindo o regulamento da União Europeia é válido para todas as empresas que detêm dados pessoais de seus clientes residentes e Hosting, independentemente de onde estejam localizadas (GDPR) General Data Protection Regulation,

Lei. 25/05/2018.
Saiba mais em: https://www.hostcuritiba.net.br/painel/termos/regulamento-geral-de-protecao-dedados.pdf
Foram aplicadas as regras e leis Nacionais para que você cliente possa ter dados assegurados e devidamente tratados pelos setores de núcleos de informações e seguidos de todas as práticas de segurança já informadas desde os procedimentos automáticos de camadas seguida de protocolos e bases jurídicas documentais. Para que os procedimentos de recuperação de dados possam ser atendidos seguindo os regulamentos e protocolos seguros, estamos agora orientados e preparados para receber seu manifesto de recuperação de modo seguro e seguindo os procedimentos declarados a seguir em conformidade para cada caso, situação de processos obrigatórios a seguir: PROCEDIMENTOS DE TROCA DE DADOS: Identificados os dados como alteráveis com os logs de atividades de geração de relatório para este processo a qual é por meio de entrada de seu descritivo: email@gmail.com, email@dominio.com como porta de entrada, as tratativas não são validadas para o mesmo e-mail de cadastro a qual descreve-se ou denomina: invadida / hackeada.

Portanto para qualquer assunto sobre este o departamento de abuse@hostcuritiba.net.br seguindo de seu pedido bilheteiro # ticket fará as tratativas certificando-se que todas as ações foram atendidas, e sem estes meios ou recusa, pode levar o domínio e dados a suspensão de conta ou cancelamento de serviços por não atender os critérios básicos e conceitos de segurança para a conta e para os servidores de tratamento sobrecarregando o serviço de acessos anônimos de ofuscação a qual nossa política de conteúdos e dados são avaliados e tratados de acordo com casa caso ou situação.

7. PROCEDIMENTOS PARA DOMÍNIOS INTERNACIONAIS

Para recuperação de dados de acesso envolvidos com domínios internacionais estes se não registrados pelo provedor e cuja proteção ID ativadas, o usuário solicitando deverá entrar em contato com o NIC de registro internacional ou o usuário a quão iniciou o pedido de registro para que este fornecer o código de transferência EPP.

O código EPP significa Extensible Provisioning Protocol, "EPP-Key", também chamado de código de autorização de domínio, é necessário para transferir seu domínio para outro host. Para consegui-lo, você deverá entrar em contato com a registradora atual do seu domínio para solicitar. Munido de seu código EPP, este deverá ser informado pelo ticket de tratamento para que possamos iniciar a transferência deste domínio para nosso ICAN/NIC de registro e certificar do usuário de registro original e suas documentações a seguir: 1. Código de autorização EPP

2. Documento de registro RG, cópia escaneada sem cortes e legítima Frente e Verso 3. Documento CPF cópia escaneada e sem cortes, Frente e Verso 4. Documento comprovante de residência no nome, Água, Luz, Conta Bancária ou títulos 5. Documentos assinados em conformidade com o Registro RG para cada cópia. Após todas as documentações já disponíveis, anexar este no pedido de ticket já em processo aguardando o prazo de autoridades de trocas dos domínios que podem levar de 24 horas até 7 dias.

8. PROCEDIMENTOS PARA DOMÍNIOS NACIONAIS

Para recuperação de dados de acesso envolvido com domínios Nacionais, estas controladas pela NIC de registro nacional, REGISTRO-BR https://registro.br/ as tratativas são em conformidade com a base de dados a seguir: Solicitar a Registram-te NIC registro br via Carta gerada pelo próprio sistema com o pedido de DELEGAÇÃO de ID Entidade da atual para a ID Entidade do Provedor: **GMDSA19** cujo após tratativa, este delegará o usuário com novo e-mail devidamente seguro e devolvida as delegações para o novo ID do cliente proprietário com as seguintes documentações:

1. Delegação de Entidade ID para a Provedora
2. Documento de registro RG, cópia escaneada sem cortes e legítima Frente e Verso
3. Documento CPF cópia escaneada e sem cortes, Frente e Verso
4. Documento comprovante de residência no nome, Água, Luz, Conta Bancária ou títulos
5. Documentos assinados em conformidade com o Registro RG para cada cópia Sobre a transferência de titularidade:
https://registro.br/ajuda.html?secao=ProcedimentosAdministrativos#d01

9. PROCEDIMENTO DE TROCA POR PEDIDO DE RECURSO

O que é pedido de recurso? Para procedimentos de trocas de dados por pedido de recurso o usuário deverá conter de acesso legítimo da conta de cadastro @e-mail do cadastro a qual este deverá informar o acesso credenciais senhas para que possamos conectar-se em seu e-mail, indicar as medidas de proteção e auditoria na conta. O cliente tendo recuperado o e-mail do cadastro a qual cujo descreve-se como: invadido / hackeado, o cliente pode desconsiderar todos os processos anteriores, uma vez que este será novamente autenticado e conformado a legitimidade da conta já cadastrada.

Nota: se o cliente não consegue acessar sua conta de cadastro, ou recuperar o acesso, e validado os procedimentos acima sobre as documentações e processos devidos para análise e liberação do domínio. Procedimentos para recuperação de contas:

1. Recuperar conta Gmail: https://support.google.com/accounts/answer/7682439?hl=pt-BR
2. Recuperar sua conta Microsoft: https://support.microsoft.com/pt-br/help/2675025
Pelo prazo de 15 dias todas as tratativa devem ser atendidas para que o pagamento do domínio, boleto e notas oficiais possam ser novamente entregues a este e-mail seguindo os critérios de segurança, estes não identificado ações em até (15) dias a parti da data protocolada # ticket, poderá suspender o domínio, hospedagem e dados removidos do servidor seguindo o contrato de prestação de serviços em:
https://www.hostcuritiba.net.br/painel/termos.php Para qualquer outra eventualidade ou procedimentos administrativos o cliente fica ciente que todos os meios de autenticações, homologações de base documentais e jurídicas seguem de acordo com os temos de responsabilidades devidamente descritas em:
https://www.hostcuritiba.net.br/painel/termos/termos-de-uso-hostcuritiba.pdf

FORO DE ELEIÇÃO 307
As partes elegem o foro da cidade de Curitiba para dirimir todas as dúvidas ou litígios resultantes da execução do presente.

HOSTCURITBA – HOSPEDAGEM DE SITES.
CNPJ: 20.962.496/0001-91

Para o esclarecimento de possíveis dúvidas em relação à terminologia técnica utilizada na internet que possa ser relevante para a interpretação do presente contrato prevalecerão as definições constantes do glossário existente nos sites:
Provedora: https://www.hostcuritiba.net.br
Institucional: https://www.hostcuritiba.com.br

HOSTCURITIBA – Hospedagem Security Central do Cliente (41) 3014-8891
Curitiba, 15 de Janeiro 2020.