POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

BRASIL GLOBALTECH LTDA

Sumário

CONSIDERAÇÕES INICIAIS

“Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio” (ABNT NBR ISO/IEC 17799:2005).

Para que toda a informação que circula possa servir somente ao seu propósito, que é o de informar, sem prejudicar quaisquer pessoas ou instituições, é necessário a gestão segura dos recursos disponíveis em tecnologia da informação.

- Tomando como base os princípios de segurança da informação, a MANAGERONE, por meio desse documento, procura adotar procedimentos padrões, de modo a contribuir de forma positiva com a:
- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas; e
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

APLICAÇÃO

Entende-se por Política de Segurança da Informação Digital da MANAGERONE, o conjunto de critérios e procedimentos de segurança, elaborados, implantados, divulgados e em contínuo processo de monitoração, visando a confidencialidade, a integridade e a disponibilidade da informação. As presentes normas aplicam-se aos empregados, comissionados, estagiários e terceiros autorizados e todos aqueles que, uma vez autorizados, venham a ter acesso aos recursos informatizados.

A área de Tecnologia da Informação é a responsável pela salvaguarda dos dados da organização, mas, o processo de segurança da informação deve envolver todos os colaboradores, independente do nível hierárquico, posto que, de posse de uma informação específica qualquer pessoa pode, por descuido e/ou com má intenção, se tornar um agente de divulgação não autorizada.

Diante do exposto, a Política da Segurança da Informação vem propor uma Gestão de Segurança da Informação baseada em controles e procedimentos técnicos, considerando e promovendo o comportamento dos colaboradores de forma que possa aplicar a tecnologia adequada em todo o processo e atingir efetividade em seu objetivo: entender o negócio e aplicar segurança a ele.

Não adianta a área da Tecnologia da Informação impor controles e medidas técnicas se não existir a participação dos colaboradores, de nada vale a implantação de barreiras e portas de controle de acesso eletrônico se um funcionário, que tem acesso legítimo a determinada área restrita, resolve divulgar informações confidenciais que estavam devidamente protegidas nesta área.

ESCOPO

É política da MANAGERONE:

- Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação da MANAGERONE sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;
- Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: Colaboradores, terceiros contratados, fornecedores e, onde pertinente, clientes.
- Garantir a educação e a conscientização sobre as práticas de segurança da informação adotadas pela MANAGERONE para Colaboradores, terceiros contratados, fornecedores e, onde pertinente, clientes.
- Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;
- Tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas;
- Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;
- Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

POLÍTICAS

SENHA

Via de regra, o acesso aos diversos serviços de informática, como sistemas, e-mail, rede local, entre outros, ocorre mediante autenticação do usuário através de seu nome de usuário (login) e senha (password). Tal processo visa garantir que o acesso à informação seja obtido apenas por pessoas autorizadas (garantia de confidencialidade).

Cada usuário é responsável pela escolha de suas senhas pessoais. Algumas recomendações importantes:

Selecione senhas de boa qualidade.

Uma senha bem elaborada reduz as chances de ser comprometida. Algumas recomendações para elaboração de senhas:

- Utilize senhas com o mínimo de: 8 caracteres, 2 letras maiúsculas, 1 letra minúscula, 1 número, 2 símbolos: @#$%.
- Não elabore senhas baseadas em informações pessoais, como nomes, sobrenomes, número de documentos, placas de carros, telefones e datas;
- Não elabore senhas baseadas em palavras que constem no dicionário de qualquer idioma;
- Não elabore senhas com caracteres repetidos ou seqüenciais. Ex.: aa22, abcde, ab123;
- Não elabore senhas com caracteres seguidos no teclado do computador. Ex.: qwer, zxcv;

Nunca divulgue ou compartilhe senhas pessoais.

As senhas são utilizadas no processo de identificação do usuário perante os acessos à sistemas e serviços de informática. Sua confidencialidade é importante, de forma a evitar que terceiros acessem informações sensíveis, como e-mails e arquivos pessoais, documentos sigilosos, etc.
Cada usuário possui logins e senhas individuais, sendo proibida a divulgação ou compartilhamento de tais dados;

Altere periodicamente as senhas

Com o objetivo de assegurar a confidencialidade das mesmas. É recomendável que as senhas sejam alteradas a cada dois ou três meses no máximo;

Quando possível, não utilize senhas iguais para serviços diferentes.

Ex.: Utilize senhas distintas para cada sistema e e-mail;

Evite registrar senhas em locais inseguros

Como anotações em papel, embaixo do teclado, adesivos colados no monitor, etc.
O recomendável é apenas memorizar a senha;

Sempre altere as senhas temporárias no primeiro acesso.

Ex.: Alterar no primeiro acesso, as senhas iniciais fornecida pela TI;

Não digite senhas quando observado

Evite que outras pessoas descubram suas senhas;

Sempre altere uma senha quando suspeitar que a mesma foi descoberta.

CERTIFICADO DIGITAL

Certificado digital é um documento eletrônico que identifica pessoas e instituições, provando sua identidade e permitindo acessar serviços informatizados com a garantia de autenticidade, integridade e não-repúdio, assim como assinar digitalmente documentos.

Cada usuário é responsável pela guarda e utilização de seu certificado digital. Algumas recomendações importantes:

- **Nunca forneça o certificado digital a terceiros.**

  O certificado digital é um documento pessoal e intransferível. Assim como outros documentos pessoais, como CPF, RG e passaporte, não deve ser fornecido a terceiros por questões de segurança;

- **Aplique as recomendações descritas no item 2. Senhas para as senhas do certificado digital. Um certificado digital possui duas senhas: PIN e PUK.**

  O PIN (Personal Identification Number) é fornecido pelo usuário na utilização do certificado, como por exemplo para assinar um documento eletrônico.

  O PUK (Personal Unblocking Key) é utilizado pelo usuário para alterar o seu PIN em caso de necessidade.

NAVEGAÇÃO NA INTERNET

A internet é uma ferramenta de trabalho utilizada pelos funcionários como apoio ao desenvolvimento de suas competências e à realização de atividades profissionais. A MANAGERONE pode monitorar seu uso para eventuais perícias, identificando os usuários e quais as páginas visitadas.

O funcionário pode usar a Internet como um recurso pessoal, desde que não interfira na execução de suas atividades profissionais, em observância às políticas e normas vigentes.

O acesso à Internet deve ser feito respeitando a legislação, as políticas e normas vigentes e preservando a imagem da MANAGERONE.

Não é permitido efetuar ações que possam ser caracterizadas como violação da segurança da informação, tais como capturar ou quebrar senhas de outros usuários, efetuar varreduras na rede, invadir sites, entre outras.

O uso da rede e da Internet deve ser feito de forma a não prejudicar os serviços de rede ou as atividades de outros funcionários, dentro ou fora da rede da MANAGERONE. Se necessário, poderão ser configurados filtros de bloqueio.

Não é permitido acessar computadores, softwares, informações ou outros recursos, sem a devida autorização ou, intencionalmente, habilitar terceiros a fazerem isso. É dever dos funcionários o respeito à propriedade intelectual e aos direitos autorais.

O acesso à Internet na MANAGERONE está disponível para funcionários a partir das estações

de trabalho conectadas à rede local da empresa. Algumas recomendações quanto à utilização da Internet:

Na MANAGERONE, utilize somente os meios de acesso à internet homologados pela TI, que são a rede local e a rede sem fio da instituição. Demais formas de acesso, como modem (acesso discado), acesso sem fio fornecido por empresas (Ex.: Oi, TIM, Claro), entre outras, não devem ser utilizadas no âmbito da instituição, pois podem comprometer a segurança da rede e das informações institucionais;

Não acesse sites e serviços Internet suspeitos, como os relacionados à pornografia, software ilegal, spam, etc. Tais sites costumam ser utilizados para disseminação de vírus e roubo de informações pessoais;

Não acesse sites e serviços da internet sem relação com as atividades desempenhadas pela instituição, como sites de jogos, fóruns não profissionais, comunidades de relacionamento pessoal, bate-papo, áudio e vídeo, dentre outros, evitando assim que o desempenho do acesso Internet e serviços relacionados sejam afetados;

Não utilize softwares e serviços Internet não homologados pela TI, evitando assim que a segurança e o desempenho da rede institucional sejam afetados;

Somente envie informações pessoais através de sites seguros. Informações pessoais, como senhas e números de cartões de crédito, devem ser fornecidas somente em sites considerados seguros. Para identificar se um site é seguro, verifique se o endereço do mesmo (URL) é iniciado por https:// e se o navegador (Ex.: Internet Explorer, Firefox) exibe a figura de um cadeado fechado;

Somente acesse sites de instituições financeiras e públicas digitando o endereço diretamente no navegador, nunca clicando em outro site ou em um e-mail recebido, evitando assim que dados pessoais sejam furtados através de sites fraudulentos;

Não utilize computadores públicos ou compartilhados, como terminais em aeroportos, cafés e shopping centers, para acessar serviços disponibilizados no site da MANAGERONE, webmail, etc. Computadores compartilhados são ambientes inseguros, onde informações sigilosas podem ser obtidas por terceiros.

CORREIO ELETRÔNICO

O serviço de correio eletrônico institucional está disponível para funcionários a partir de qualquer estação com acesso à Internet. Algumas recomendações quanto à utilização do serviço de correio eletrônico:

Não abra e-mails e anexos considerados suspeitos, como os relacionados à pornografia, propagandas, correntes, arquivos executáveis, remetentes desconhecidos, dentre outros. Tais e-mails e anexos costumam ser utilizados para disseminação de vírus e roubo de informações pessoais. Caso considere um e-mail ou anexo suspeito, apague o mesmo de sua caixa postal;

Limpe periodicamente sua caixa postal, apagando e-mails antigos, spams, etc. Tal procedimento previne o não recebimento de e-mails, devido ao limite da caixa postal;

Evite enviar e-mails para um grande número de destinatários, pois tal atitude compromete o desempenho da rede local e do serviço de correio eletrônico, além de expor ao risco de o domínio da empresa ser inserido em lista de spam;

Utilize o serviço de correio eletrônico somente para fins profissionais, pois o envio de e-mails sem relação com as atividades desempenhadas pela instituição compromete o desempenho da rede local e do serviço de correio eletrônico;

Divulgue seu e-mail da MANAGERONE somente para fins profissionais, evitando informar o mesmo em sites e serviços da internet não seguros. Tal procedimento reduz o recebimento de spams, mensagens indesejadas e roubo de credenciais;

FERRAMENTA DE ANÁLISE DE E-MAILS

A MANAGERONE disponibiliza uma solução que analisa todos os e-mails que seus colaboradores recebem. Trata-se do ONINBOX que é uma camada de inteligência que alerta os usuários de e-mail através de indicadores de risco de semáforos a cada e-mail recebido sobre possíveis fraudes de personificação de marca, fraudes de pagamento e outros tipos de ataque. Realiza, portanto, a proteção e o treinamento do usuário no momento da necessidade. É a atualização dos treinamentos de phishing para avisos em tempo real.

A adoção desta solução se deve ao fato de os Gateways de segurança de e-mail (SEGs) e o treinamento de conscientização de phishing sozinhos não funcionam. Para que o processo esteja completo, uma camada de segurança de email que potencializa o treinamento tradicional através de comunicações em tempo real alertando os usuários no momento em que as ameaças surgem. É aí que o ONINBOX se encaixa e coloca em prática as melhores práticas de prevenção e detecção de ameaças por e-mail. A empresa entende que a velha política de culpar os usuários vítimas de ataques simplesmente por lhes ter fornecido treinamento não tem mais espaço em uma época em que dados tão valiosos estão sendo tratados.

Somente com um sistema inteligente que aprende como o uso e que evolui constantemente é possível lidar com as mutações dos ataques.

Cada email recebido pode conter uma ameaça.

A possibilidade de que isto realmente aconteça depende de três fatores:

- Como a mensagem foi enviada
- Quem enviou o email
- O que o email contém

TRATAMENTO DOS RISCOS DE EMAIL

INDICADORES

O ONINBOX usa um indicador bem claro composto por 3 partes para alertar os usuários sobre o risco de cada email recebido.

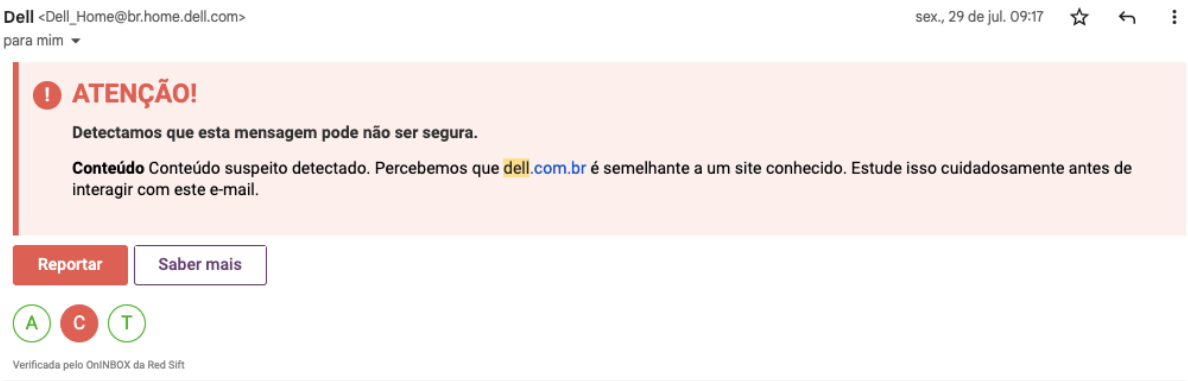
a) **Como a mensagem foi enviada** – O ONINBOX verifica se o remetente do email é quem ele diz que é avaliando os protocolos de segurança (DMARC, SPF, DKIM) que o remetente possui. Quanto maior a segurança do remetente, menor o risco que o usuário está correndo. Note que é impossível o usuário no momento em que recebe um email saber sobre o nível de segurança que o remetente possui. O ONINBOX analisa e sinaliza em tempo real tal nível de segurança, ou seja, mostra como a mensagem foi enviada, se de uma fonte segura ou de uma fonte insegura.
   Este primeiro alerta e o **A** de autenticação

b) **O que o email contém** – O ONINBOX faz a revelação de conteúdo oculto, examinando (não lendo) o conteúdo dos emails para destacar algo que possa lhe causar danos como rastreamento de pixels, URLs maliciosas ou até mesmo domínios inválidos. Isso é combinado com modelos avançados de aprendizado de máquina que capacitam o ONINBOX a analisar a linguagem e o comportamento humano. Trata-se do alerta **C** de conteúdo.

c) **Quem enviou o email** – O ONINBOX aprende sobre como você interage com as pessoas para identificar ameaças e construir sua rede confiável. É comum fraudadores enviarem e-mail através de remetentes muito semelhantes a um remetente confiável. Na correria do dia a dia acabamos não percebendo pequenas diferenças de grafia. Ao identificar situações como essa de tentativa de enganar o usuário final, o ONINBOX através do segundo alerta informa o usuário de que algo muito parecido com a sua rede de confiança apareceu no email recebido, tratado do alerta **T** (trust) de confiança.

BANNER de ameaça de e-mail

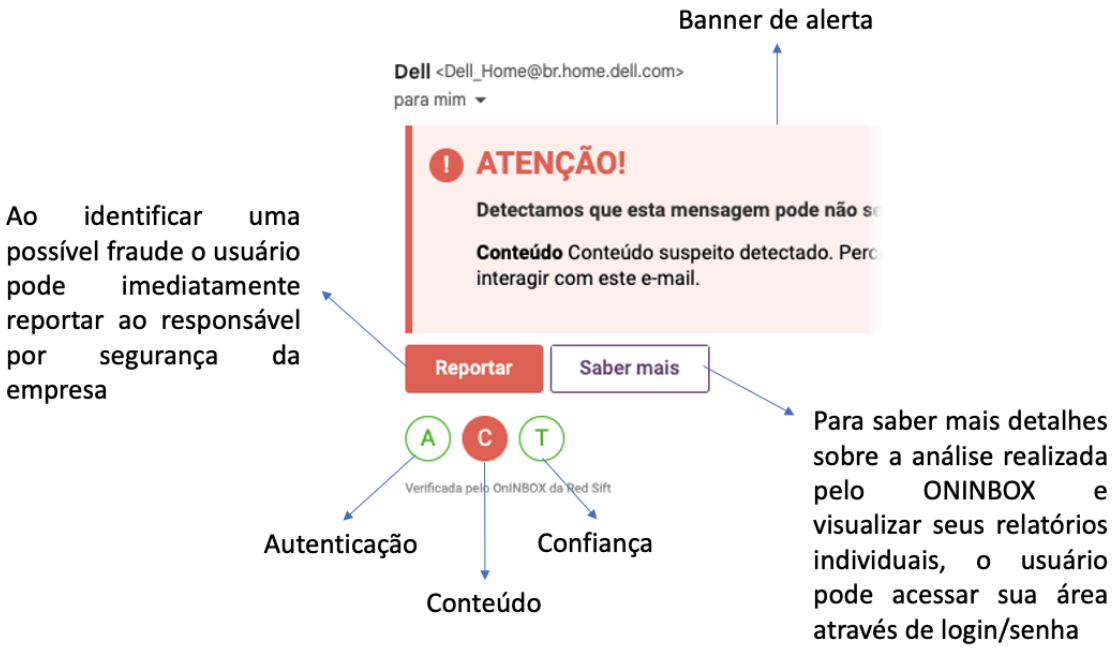
O ONINBOX dependendo da situação encontrada de nível de configuração pré-estabelecida pelo administrador, pode inserir além dos sinais A, C e T, um banner de alerta.



O Banner insere um alerta de valor imediato, passando a ser um especialista em segurança dentro de cada email. Com as informações apresentadas o usuário passa a ter um conjunto de informações que o auxiliam na tomada de decisão de acreditar no e-mail recebido ou não sob a perspectiva dos três fatores analisados.

USABILIDADE

A utilização do ONINBOX e intuitiva e contextualizada a cada e-mail conforme exemplificado na imagem:



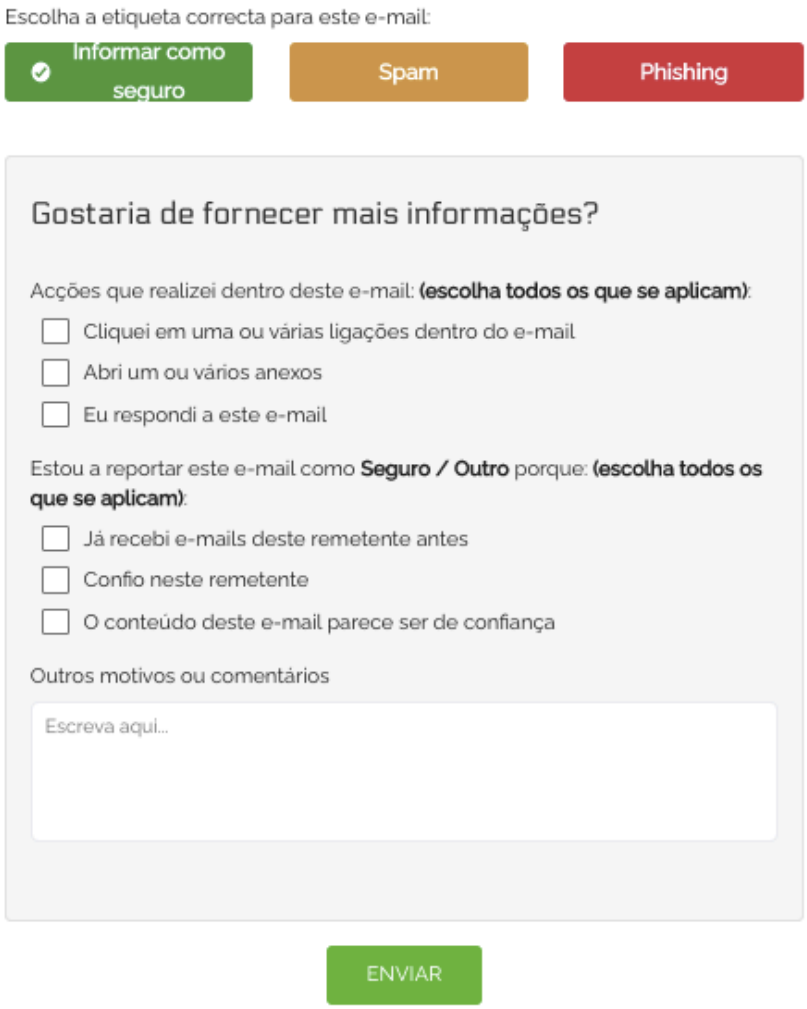
REPORTAR UM EMAIL

O usuário pode reportar um email ao administrador de segurança da empresa para que este possa revisar o conteúdo. Basta clicar no ícone 'Reportar' na própria mensagem. Na interface do usuário logado, aparecerá uma tela com opção de marcar o email como seguro, como spam ou como *phishing*.

Ao selecionar uma das três opções apresentadas, "informar como seguro", Spam ou phishing, o usuário poderá enviar mais informações escolhendo entre as opções apresentadas na caixa de seleção ou adicionando comentários explicando por que decidiram reportar este email.

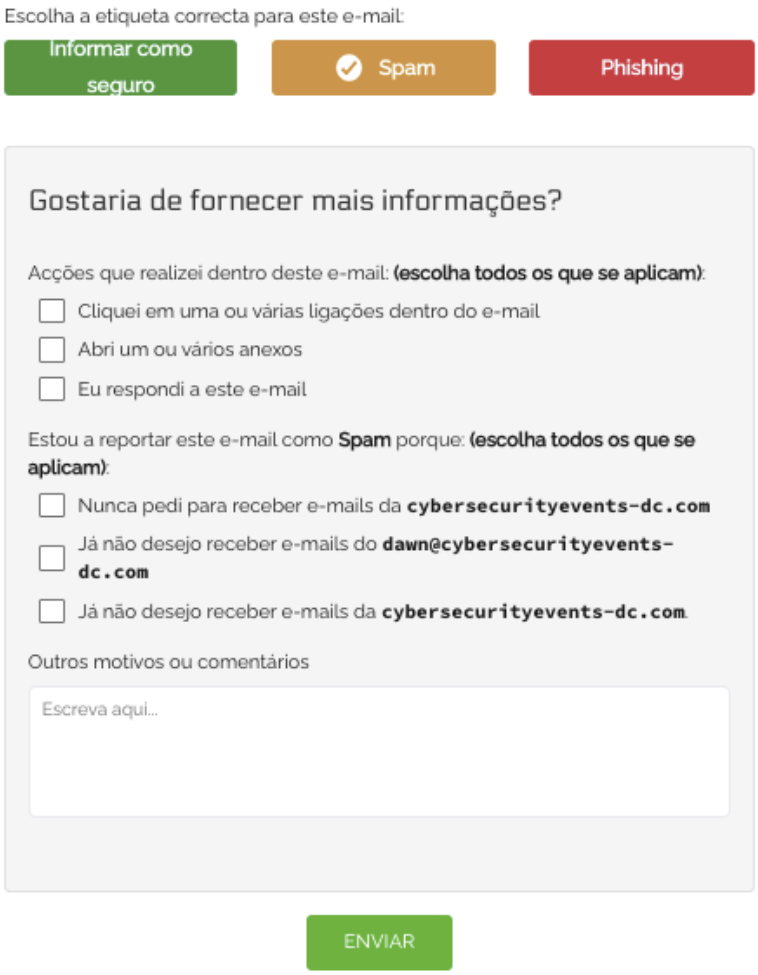
Ao escolher a opção 

, as informações apresentadas são as seguintes:


Escolha a etiqueta correcta para este e-mail:
Informar como seguro
Spam
Phishing
Gostaria de fornecer mais informações?
Acções que realizei dentro deste e-mail: (escolha todos os que se aplicam):
Cliquei em uma ou várias ligações dentro do e-mail
Abri um ou vários anexos
Eu respondi a este e-mail
Estou a reportar este e-mail como Seguro / Outro porque: (escolha todos os que se aplicam):
Já recebi e-mails deste remetente antes
Confio neste remetente
O conteúdo deste e-mail parece ser de confiança
Outros motivos ou comentários
Escreva aqui...
ENVIAR

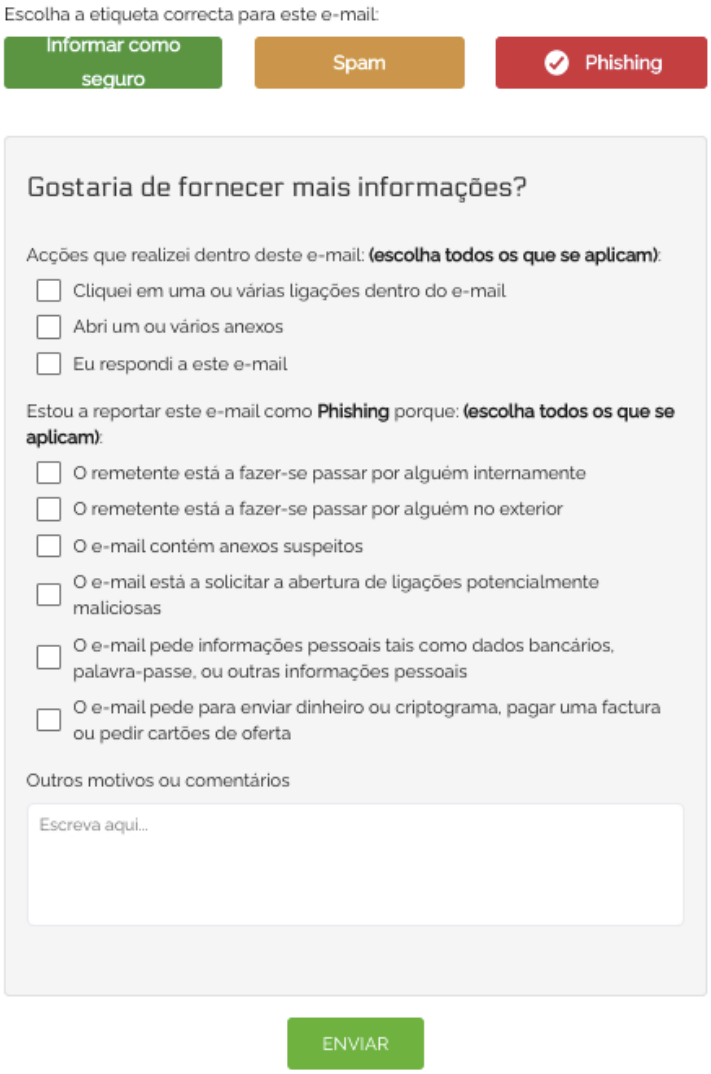
Ao escolher a opção 

, as informações apresentadas são as seguintes:

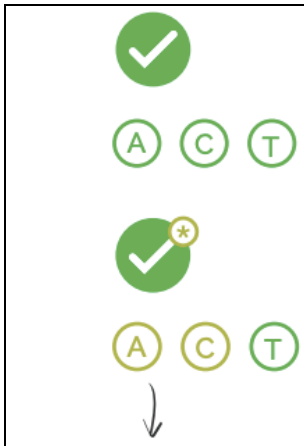


Ao escolher a opção 

, as informações apresentadas são as seguintes:



Como interpretar os alertas do ONINBOX

		
Nenhuma ação necessária	**Saber mais**	**Saber mais**
É seguro interagir com este email	Esses resultados podem melhorar. Saiba quais ações tomar	Uma ameaça foi identificada. Saiba porque você não deve interagir

USO DE DISPOSTIVIVOS MÓVEIS

A MANAGERONE utiliza em todos os seus dispositivos a ferramenta de MDM (*mobile device management*) o SOTI MobiControl.

A utilização do MDM garante que os usuários de dispositivos que pertençam a MANAGERONE aceitem o termo de uso dos dispositivos autorizando o seu devido gerenciamento.

A solução disponibiliza dentre outros, os seguintes recursos:

- Estabelecimento de políticas de senha
- Controle para que o uso do dispositivo seja somente profissional.
- Restrição de horário para acessar aplicativos
- Restrição de uso de funções
- Controle do uso de telecom
- Localização em caso de extravio
- Apagar dados em caso de extravio
- Bloqueio de compartilhamento de internet
- Uso de modo quiosque para funções específicas
- Política de atualização de Sistema operacional
- Acesso e controle remoto em caso de suporte técnico
- Restrição de navegação internet

PROTEÇÃO DE DOMÍNIO

A MANAGERONE monitora todos os seus domínios com objetivo de detectar fraudes provenientes de domínios semelhantes para evitar violações de uso de marca e ataques *phishing*.

Temos conhecimento de domínios assim que são registrados e os monitoramos. Detectamos sites hospedados destes domínios suspeitos e eventual utilização de nosso logotipo. Após constatação de fraude efetuamos a derrubada dos sites e domínios fraudulentos.

Além monitorar domínios semelhantes, protegemos nosso próprio domínio com os protocolos disponíveis: SPF, DKIM e DMARC.

DADOS DA EMPRESA

RAZÃO SOCIAL: BRASIL GLOBALTECH LTDA.
CNPJ: 21.775.339/0001-30
RUA VERBO DIVINO, 2001, CONJ. 912, BLOCO B, CHÁCARA SANTO ANTÔNIO, SÃO PAULO – SP - 04.719-002

ENCARREGADO DE DADOS

CLAYTON DE SOUZA SILVA
OAB/PR: 109005
CLAYTON@MANAGERONE.COM.BR