COMPLEXO
DE SAÚDE
SÃO BERNARDO
DO CAMPO

FLS 150
VISTO

São Bernardo do Campo, 28 de julho de 2023

Sumário

FUNDAÇÃO DO ABC

Objetivo:

Este documento visa introduzir o conhecimento sobre Phishing, realizar o entendimento da ocorrência solicitada pelo **Departamento de Compras e Contratos** sobre um remente específico de e-mail, não entregue na caixa postal de destino.

Introdução:

A Segurança da Informação é um ramo da Tecnologia da Informação e Comunicação que visa defender e assegurar dados e informações em cinco pilares:

Confidencialidade:

A confidencialidade é o pilar que diz que toda a informação deve ser compartilhada e acessada apenas as pessoas para quem se destinam. Ou seja, apenas pessoas autorizadas podem ter acesso a essa informação ou dado. Uma quebra da confidencialidade significa um vazamento ou exposição da informação, que pode causar um prejuízo direto ou indireto, financeiro ou de reputação.

Integridade:

Este pilar diz respeito ao processo de entrada e de saída da informação durante seu fluxo e tempo de atividade. Podemos definir que a informação que entra no fluxo, deve ser integralmente a mesma que é comunicada por todo o percurso de seu fluxo até o final, sem que haja alterações ou modificações. Sua principal característica é a garantia que o arquivo, dado ou informação não foi alterado garantindo assim sua confiança, permitindo uma tomada de decisão com maior clareza e transparência.

Disponibilidade:

A disponibilidade apresenta como sua característica principal, manter o arquivo, dado ou informação operacional e acessível às pessoas autorizadas e funcional durante todo o tempo do fluxo da informação, sem interrupções, propositais ou não, evitando assim um tempo maior que o previso para o fluxo da informação. A indisponibilidade ou downtime causa grandes prejuízos para as empresas e perda de oportunidades de negócios.

Irretratabilidade:

Irretratabilidade (ou não-repúdio) a não contestação da autoria do arquivo, dado ou informação em questão. Isso pode ser exemplificado com o a comprovação que quem realizou uma alteração em plataforma ou sistema, impedindo que haja rejeição da ação ou acordos.

Autenticidade:

De modo geral, autenticidade é o registro da autoria de origem e últimas alterações realizadas sobre o dado, informação ou arquivo. Pode ser feito via documentações, formalizações ou tecnologias diversas como: log, reconhecimento facial, leitura digital etc. Uma falha nos protocolos de autenticidade representa uma falha na autenticidade de segurança que pode ocasionar fraudes ou invasões.

São nesses cinco pilares que baseamos nosso critério de segurança da informação. Em constante processo de melhoria contínua, baseada no PDCA (Plan-Do-Check-Action) procuramos investir continuamente na contratação, desenvolvimento e pesquisa das melhores soluções e fornecedores para manter o ambiente CSSBC distante de possíveis riscos materializados na SI (segurança da informação).

O departamento de Tecnologia da Informação e Comunicação, baseado nas boas práticas da segurança da informação, citamos abaixo algumas das medidas de segurança adotadas:

Política de Tecnologia da Informação ou PSI:

A política "Política de Uso dos Recursos de Tecnologia da Informação", atualmente vigente, é a equivalente à Política de Segurança da Informação nesta instituição. Ela encontra-se publicada na Intranet da instituição, de acesso a todos os colaboradores.

As informações contidas no documento preveem:

- papeis e responsabilidades;
- fluxo de autorização de acesso e transferências;
- fluxo de desligamentos;
- uso das estações de trabalho;
- propriedade intelectual;
- segurança e integridade dos dados;
- compartilhamento de dados;
- informações sobre backup, cópias locais e uso de cloud (nuvem);
- instalações de programas;
- uso da internet;
- uso da intranet;
- uso de impressoras;
- uso de e-mail;
- uso de notebooks;
- rede wi-fi;
- programas de comunicação;
- uso de aparelhos celulares e móveis;
- uso da telefonia fixa;

Possuímos em processo de revisão a "Política de Segurança da Informação", atualização da que "Política de Uso dos Recursos de Tecnologia da Informação". Tem por objetivo possibilitar o gerenciamento da segurança de informação na organização, estabelecendo regras e padrões atualizados para proteção da informação. Todos os funcionários serão capacitados e treinados após a revisão e aprovação da nova política.

Termo de confidencialidade e sigilo:

Termo de confidencialidade e sigilo, assinado por todos os funcionários da instituição, no momento de sua integração através do departamento de RH. Este termo representa um documento firmado entre instituição e colaborador para manter determinadas informações citadas no termo, em sigilo e confidencialidade, mesmo após interrupção do contrato de trabalho.

Controle de Acessos Externos e Internos:

Todas as unidades hospitalares possuem controle de acesso através de crachás ou reconhecimento facial. Estas tecnologias garantem acesso controlado na entrada e setores utilizando a metodologia de "algo que você possui" ou "quem você é". O monitoramento via câmeras e agentes de segurança patrimonial 24 horas, garantem a integridade física da instituição. As tecnologias empregadas são de última geração e alta resolução o que garante ótima gestão e monitoramento.

Antivírus:

Utilizamos umas das tecnologia de antivírus líder de mercado. Solução com gerenciamento centralizada, garantindo uniformidade e atualizações centralizadas. Centralização de políticas, gestão de dispositivos, bloqueio de ameaças, além de extração e emissão de relatórios diários de status da solução.

Uma gestão organizada garante respostas rápidas aos incidentes ligados aos vírus, malwares, adwares e outras ameaças que possam colocar em risco o patrimônio digital da instituição.

Registros de Logs:

Possuímos registros de logs em diversos sistemas, softwares, hardwares e appliances, garantindo assim uma análise dos registros para diagnósticos preventivos e corretivos.

Controles de Acessos Lógicos:

Os sistemas utilizados nas unidades de saúde possuem controle de acessos lógicos de usuário e senha, além de controle de acessos de acordo com o método de acesso, local de acesso, perfil adotado e a função de cada usuário.

O acesso à internet é um item protegido pelos perfis de acesso e restrito apenas as pessoas que realmente necessitam dessa ferramenta em suas funções.

Da mesma maneira podemos citar o acesso às pastas de rede, sistemas, rede sem fio, impressoras, armazenamentos cloud, entre outros.

Toda a criação de acesso, remoção e alteração é controlada rigorosamente através de fluxo, desde a contratação e desligamento, com o departamento de recursos humanos. A liberação de acesso somente é permitida após aprovação do gestor do departamento através da ferramenta de chamado.

Banco de Dados:

Utilizamos ERP conceituado na área da saúde, amplamente utilizado em hospitais e de longa data de mercado.

Os dados são armazenados em banco de dados relacional de conceituada empresa, alto poder processamento e desempenho, alta capacidade e protegido através de criptografia e armazenado em cloud líder de mercado.

A estrutura cloud possui monitoramentos de links, backup, gestão de capacidade, saúde de servidores e de controles rígidos de gestão de acesso.

Backups:

Realizamos backups da infraestrutura, utilizando software de mercado, não open source, de alta performance, em ambiente seguro e protegido.

Firewall:

Utilizamos solução de mercado, não open source (código aberto), com atualizações de segurança garantidas durante a vigência da vida útil do produto. As regras são baseadas em bloqueio. Não havendo incidentes relacionados a invasões ou falso positivo de acessos conhecidos.

Redundância de saídas e regras rígidas e revisadas frequentemente, garantem gestão, segurança e continuidade do negócio.

Sistema de Monitoramento contra ameaças:

Possuímos contrato com empresa terceira especializada na atividade de monitoramento em infraestrutura, que realiza a atividade de monitoramento cloud, além de serviço de monitoramento da infraestrutura, verificando a saúde dos servidores, links, gestão de capacidade, saúde de servidores e gestão de acessos. Atuamos ativamente em qualquer mudança de estado nos itens de configuração (IC).

Sistema de Chamados e Incidentes

Possuímos ferramenta de registro de chamado para controlar abertura de requisições, incidente, problemas e mudanças. Através dela e do cadastro prévio de SLA de categorizado por tipo de ticket. O colaborador pode fazer a abertura de chamado e acompanhamento da demanda.

Atualizações de Software e Sistemas

Central unificada para atualização de Sistemas Operacionais. Solução própria do desenvolvedor, realiza a verificação, indicando itens para serem atualizados que podem ou não ser aprovados para aplicação em demanda.

Atualizações centralizadas para os sistemas ERPs e outros softwares sempre fornecidos pelos desenvolvedores e testados em ambiente de homologação.

E-mails e Comunicação

A comunicação é realizada através de Intranet, protegida por usuário e senha e acesso de acordo com o perfil. Outra ferramenta de comunicação é o e-mail, totalmente integrado com a rede

corporativa e profissional. Possui ferramentas avançadas de detecção de documentos com informações sensíveis e AntiSpam e detecção de arquivos maliciosos.

Assinatura Digital

Utilizamos assinatura digital através de certificada compatível com o ERP hospitalar. Essa ferramenta é utilizada por médicos e enfermeiras garantindo o não-repúdio, comprometimento e responsabilidade na emissão de informações para os pacientes.

Outro sistema utilizado é o de assinatura digital em documentos através de certificado digital gerado na própria ferramenta. Essa ferramenta garante, além do não-repúdio, a aprovação ou reprovação de documentos online pelas partes interessadas. Outra vantagem é a manutenção de documentos numa única ferramenta, com as assinaturas já realizadas para futura consulta.

O que é Phishing?

Segundo a Malwarebytes em seu site:

"Phishing é o crime de enganar as pessoas para que compartilhem informações confidenciais como senhas e número de cartões de crédito. Como em uma verdadeira pescaria, há mais de uma maneira fisgar uma vítima, mas uma tática de phishing é a mais comum. As vítimas recebem um e-mail ou uma mensagem de texto que imita (ou "engana") uma pessoa ou organização em que confiam, como um colega de trabalho, um banco ou um órgão governamental. Quando a vítima abre o e-mail ou o texto, eles encontram uma mensagem assustadora que induz a deixar o bom senso de lado ao deixá-los com medo. A mensagem exige que a vítima acesse um website e execute uma ação imediata ou assuma um risco por algum tipo de consequência.

Se os usuários mordem a isca e clicam no link, eles enviam uma imitação de um website legítimo. A partir daí, eles pedem para fazer o login com nome de usuário e senha. Se forem ingênuos o bastante para obedecer, as informações de acesso são enviadas aos ladrões que as usam para roubar identidades, roubam contas bancárias e vendem os dados pessoais no mercado negro."

(fonte:

Ou seja, é o ato do infrator remente de tentar enganar a vítima destinatária através de convencimento ou de oportunidade para que a mesma venha por vontade própria iniciar uma ação que pode acarretar em um prejuízo pessoal ou corporativo. Segundo Adam Kujawa, diretor do Malwarebytes Labs, "Phishing é o tipo mais simples de ciberataque e, ao mesmo tempo, o mais perigoso e eficiente porque ele ataca o computador mais vulnerável e poderoso do planeta: a mente humana." Não se trata apenas de uma ferramenta, mas sim de um conjunto de estratégias e táticas de "fisgar" a vítima.

"Em 2017, um phishing scam maciço induziu os departamentos de contabilidade do Google e do Facebook a transferirem dinheiro, um total de mais de $100 milhões, para contas em bancos no exterior sob o controle de um hacker." – cita a Mawarebytes em seu site.

Segundo a própria Microsoft ( ), algumas maneiras de identificar um possível Phishing, seriam:

- Chamada urgente à ação ou ameaças - Suspeite de e-mails que afirmam que você deve clicar, ligar ou abrir um anexo imediatamente. Muitas vezes, eles alegarão que você tem que agir agora para reivindicar uma recompensa ou evitar uma penalidade. Criar um falso senso de urgência é um truque comum de ataques de phishing e golpes. Eles fazem isso para que você não pense muito sobre isso ou consulte um conselheiro confiável que pode avisá-lo.

  Dica: Sempre que você vir uma mensagem pedindo uma ação imediata, pare um pouco e observe cuidadosamente a mensagem. Você tem certeza que ela é real? Reduza a velocidade e fique mais seguro.

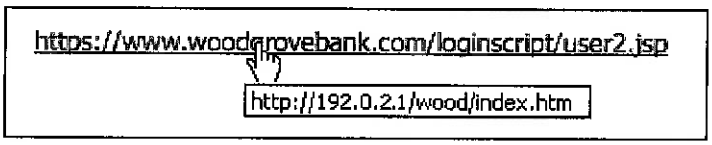
- Remetentes novos ou não frequentes - Embora não seja incomum receber um e-mail de alguém pela primeira vez, especialmente se o remetente não pertence à sua organização, isso poderá ser um sinal de phishing. Quando você recebe um e-mail de alguém que não reconhece ou que o Outlook identifica como um novo remetente, tire um momento para examiná-lo com cuidado.

- Ortografia e gramática ruim – empresas e organizações profissionais geralmente têm uma equipe editorial para garantir que os clientes obtenham conteúdo profissional e de alta qualidade. Se uma mensagem de e-mail apresentar erros ortográficos ou gramaticais óbvios, pode ser um golpe. Às vezes, esses erros são o resultado de uma tradução inadequada de um idioma estrangeiro e, às vezes, são deliberados na tentativa de escapar dos filtros que tentam bloquear esses ataques.

- Saudações genéricas - uma organização que trabalha com você deve saber o seu nome e, atualmente, é fácil personalizar um e-mail. Se o e-mail começar com um genérico "Prezado senhor ou senhora", isso é um sinal de alerta de que pode não ser realmente o seu banco ou site de compras.

- Domínios de e-mail incompatíveis - Se o e-mail afirma ser de uma empresa respeitável, como a Microsoft ou seu banco, mas o e-mail está sendo enviado de outro domínio de e-mail como Gmail.com ou microsoftsupport.ru provavelmente é um golpe. Também esteja atento a erros de ortografia muito sutis no nome de domínio legítimo. Por exemplo, micros0ft.com, onde o segundo "o" foi substituído por um 0 ou rnicrosoft.com, onde o "m" foi substituído por um "r" e um "n". Esses são truques comuns de golpistas.

- Links suspeitos ou anexos inesperados - Se suspeitar que uma mensagem de e-mail é uma fraude, não abra nenhum link ou anexo que houver. Em vez disso, passe o mouse sobre o link, mas não clique, para ver se o endereço corresponde ao link que foi digitado na mensagem. No exemplo a seguir, descansar o mouse sobre o link revela o endereço web real na caixa com o plano de fundo amarelo. Observe que a cadeia de caracteres de números não se parece nada com o endereço Web da empresa.



De que maneira o CSSBC (Complexo de Saúde São Bernardo do Campo) protege seus colaboradores de ataques phishing?

Vimos a complexidade de uma análise de phishing para um ser humano, pois decorre de diversas interpretações e decisões de todo um conteúdo, assim utilizamos comumente ferramentas e instrumentos que auxiliam no desejado "filtro" anti-phishing, classificando de forma automatizada as decisões de bloqueio ou não do conteúdo.

A área de Gestão de Tecnologia da Informação e Comunicação (Gestic) investe e utiliza as próprias barreiras de segurança embarcadas na solução Microsoft Exchange Online (solução de e-mail), somada às ferramentas inclusas no Microsoft 365 e em última instância o antivírus local, para realizar a proteção anti-phishing. Abaixo explicaremos algumas barreiras de proteção aplicadas no CSSBC.

Barreiras de Proteções

AntiSpam:

De acordo com a Microsoft em seu site:

"A maioria dos spams é excluída por meio da filtragem de conexão na borda do serviço, que se baseia no endereço IP do servidor de e-mail de origem. Políticas anti spam (também conhecidas como políticas de filtro de spam ou políticas de filtro de conteúdo) inspecionam e classificam as mensagens como spam, spam, spam de alta confiança, phishing ou phishing de alta confiança.
As políticas anti-spam são usadas nas políticas de segurança predefinidas Standard e Strict. Você pode criar políticas anti-spam personalizadas que se aplicam a grupos específicos de usuários. Há também uma política anti-spam padrão que se aplica a todos os destinatários que não são especificados nas políticas de segurança predefinidas Standard e Strict ou em políticas personalizadas.
Por padrão, as mensagens identificadas como spam são movidas para a pasta Junk Email pela política de segurança predefinida Standard, políticas anti-spam personalizadas (configuráveis) e a política anti-spam padrão (configurável). Na política de segurança predefinida estrita, as mensagens de spam são colocadas em quarentena."

(Fonte: https://learn.microsoft.com/pt-br/microsoft-365/security/office-365-security/anti-spam-protection-faq?view=o365-worldwide)

AntiMalware:

Segundo a Microsoft em seu site:

Em organizações do Microsoft 365 com caixas de correio no Exchange Online ou em um cliente independente da EOP (Proteção do Exchange Online), ou em organizações sem caixas de correio do Exchange Online, as mensagens de e-mail de entrada serão automaticamente protegidas contra spam pela EOP. Algumas das principais categorias de malware são:

- *Vírus* que infectam outros programas e dados e se espalham pelo computador ou rede à procura de programas para infectar.
- *Spyware* que coleta suas informações pessoais, como informações de entrada e dados pessoais, e envia-as de volta para seu autor.
- *Ransomware* que criptografa seus dados e exige pagamento para descriptografá-los. O software anti-malware não ajuda você a descriptografar arquivos criptografados, mas pode detectar a carga de malware associada ao ransomware.

O EOP oferece proteção contra malware em várias camadas projetada para capturar todos os malwares conhecidos no Windows, Linux e Mac que viajam para dentro ou fora de sua organização. As opções a seguir ajudam a fornecer proteção antimalware:

- *Defesas em camada contra malware*: vários mecanismos de verificação antimalware ajudam a proteger contra ameaças conhecidas e desconhecidas. Esses mecanismos incluem detecção heurística avançada a fim de fornecer proteção mesmo durante os estágios iniciais de um surto de malware. Essa abordagem multimotor tem sido mostrada para fornecer significativamente mais proteção do que usar apenas um mecanismo anti-malware.
- *Resposta a ameaças em tempo real:* durante alguns surtos, a equipe anti-malware pode ter informações suficientes sobre um vírus ou outra forma de malware para escrever regras políticas sofisticadas que detectam a ameaça, mesmo antes de uma definição estar disponível de qualquer um dos mecanismos de verificação usados pelo serviço. Essas regras são publicadas na rede global a cada 2 horas para fornecer à sua organização uma camada extra de proteção contra ataques.
- *Implantação rápida de definição anti-malware:* a equipe anti-malware mantém relações próximas com parceiros que desenvolvem mecanismos anti-malware. Como resultado, o serviço pode receber e integrar definições e patches de malware antes de serem liberados publicamente. Nossa conexão com esses parceiros muitas vezes nos permite desenvolver nossos próprios remédios também. O serviço busca definições atualizadas para todos os mecanismos antimalware a cada hora.

(Fonte: https://learn.microsoft.com/pt-br/microsoft-365/security/office-365-security/anti-malware-protection-about?view=o365-worldwide)

Anti-Phishing:

Novamente, de acordo com a Microsoft:

Phishing é um ataque por email que tenta roubar informações confidenciais em mensagens que parecem ser de remetentes legítimos ou confiáveis. Há categorias específicas de phishing. Por exemplo:

- *O phishing de lança* usa conteúdo personalizado e focado que é especificamente adaptado para os destinatários de destino (normalmente, após o reconhecimento nos destinatários pelo invasor).
- *Whaling* direcionado a executivos ou outros destinos de alto valor dentro de uma organização para efeito máximo.
- *O BEC (compromisso de email comercial)* usa remetentes confiáveis forjados (agentes financeiros, clientes, parceiros confiáveis etc.) para enganar os destinatários para aprovar pagamentos, transferir fundos ou revelar dados do cliente.
- *Ransomware* que criptografa seus dados e exige pagamento para descriptografá-los quase sempre começa em mensagens de phishing. A proteção anti-phishing não pode ajudá-lo a descriptografar arquivos criptografados, mas pode ajudar a detectar as mensagens iniciais de phishing associadas à campanha de ransomware.

Com a complexidade crescente dos ataques, é até difícil para usuários treinados identificar mensagens de phishing sofisticadas. Felizmente, Proteção do Exchange Online (EOP) e os recursos adicionais em Microsoft Defender para Office 365 podem ajudar.

Proteção anti-phishing em EOP

As organizações do Microsoft 365 com caixas de correio em organizações EOP Exchange Online ou autônomas sem caixas de correio Exchange Online contêm os seguintes recursos que ajudam a proteger sua organização contra ameaças de phishing:

- *Inteligência falsa*: use o insight de inteligência falsa para examinar remetentes falsificados detectados em mensagens de domínios externos e internos e permitir ou bloquear manualmente os remetentes detectados.
- *Políticas anti-phishing no EOP:* ativar ou desativar a inteligência falsa, ativar ou desativar indicadores de remetente não autenticados no Outlook e especificar a ação para remetentes falsificados bloqueados.
- *Honre a política DMARC do remetente quando a mensagem for detectada como falsificação:* controle o que acontece com as mensagens em que o remetente falha nas verificações explícitas do DMARC e a política DMARC é definida como p=quarantine ou p=reject.
- *Permitir ou bloquear remetentes falsificados na Lista de Permissões/Blocos do Locatário:* quando você substitui o veredicto no insight de inteligência falsa, o remetente falsificado se torna uma entrada manual de permissão ou bloqueio que aparece apenas na guia **Remetentes Falsificados** na página **Permitir/Bloquear Listas de Locatários** em https://security.microsoft.com/tenantAllowBlockList?viewid=SpoofItem. Você também pode criar manualmente entradas de permissão ou bloqueio para remetentes falsificados antes que eles sejam detectados pela inteligência contra falsificação.
- *Autenticação de email implícita:* o EOP aprimora as verificações padrão de autenticação de e-mail para e-mail de entrada (SPF, DKIM e DMARC com reputação de remetente, histórico do remetente, histórico do destinatário, análise comportamental e outras técnicas avançadas para ajudar a identificar remetentes forjados.

(Fonte: https://learn.microsoft.com/pt-br/microsoft-365/security/office-365-security/anti-phishing-protection-about?view=o365-worldwide)

Caixa de quarentena:

No Microsoft 365 organizações com caixas de correio em organizações Exchange Online ou EOP (Proteção do Exchange Online autônomo) sem caixas de correio Exchange Online, a quarentena está disponível para conter mensagens potencialmente perigosas ou indesejadas.
Se uma mensagem detectada é colocada em quarentena por padrão depende dos seguintes fatores:

- O recurso de proteção que detectou a mensagem. Por exemplo, as seguintes detecções são sempre colocadas em quarentena:
- Detecções de malware por políticas anti-malware e políticas de Anexos Seguros, incluindo proteção interna para anexos seguros.
- Detecções de phishing de alta confiança por políticas anti-spam.

As ações padrão para recursos de proteção no EOP e Defender para Office 365, incluindo políticas de segurança predefinidas, são descritas nas tabelas de recursos em configurações recomendadas para segurança de EOP e Microsoft Defender para Office 365.

As políticas de proteção para recursos com suporte têm uma ou mais políticas de quarentena atribuídas a elas (cada ação dentro da política de proteção tem uma atribuição de política de quarentena associada).

As políticas de quarentena definem o que os usuários podem fazer ou não com mensagens em quarentena e se os usuários recebem notificações de quarentena para essas mensagens. Para obter mais informações, consulte Anatomia de uma política de quarentena.

As políticas de quarentena padrão atribuídas aos veredictos do recurso de proteção impõem as funcionalidades históricas que os usuários recebem para suas mensagens em quarentena (mensagens em que são destinatários). Para obter mais informações, consulte a tabela em Localizar e liberar mensagens em quarentena como usuário no EOP. Por exemplo, somente os administradores podem trabalhar com mensagens que foram colocadas em quarentena como malware ou phishing de alta confiança. Por padrão, os usuários podem trabalhar com suas mensagens que foram colocadas em quarentena como spam, em massa, phishing, paródia, representação do usuário, representação de domínio ou inteligência de caixa de correio.

(Fonte; https://learn.microsoft.com/pt-br/microsoft-365/security/office-365-security/quarantine-about?view=o365-worldwide)

No CSSBC utilizamos esse recurso para classificações de alto risco, padrão Microsoft:

-Conteúdo com Malware;

-Conteúdo com Phishing de Alta Confiança;

Outros e-mails de menor classificação, são enviados para o Lixo Eletrônico.

Lixo eletrônico;

Filtro Email de Lixo eletrônico do Outlook usa sua própria tecnologia de filtro SmartScreen para identificar e mover spam para a pasta Junk Email. Portanto, o Outlook Junk Email Filter é capaz de usar a coleção de listas de segurança da caixa de correio e sua própria classificação de spam para mover mensagens para a pasta Junk Email.

(Fonte: https://learn.microsoft.com/pt-br/microsoft-365/security/office-365-security/configure-junk-email-settings-on-exo-mailboxes?view=o365-worldwide)

Antivírus

A ferramenta de Endpoin Security, que garante proteção contra links maliciosos e arquivos maliciosos oriundos de sites, rede local e e-mail, que possam conter ameaças ou exploits (programas que tem como objetivo se aproveitar de pontos fracos de software).

Firewall

O firewall utilizado no CSSBC garante acesso restrito e bloqueado aos endereços maliciosos contidos em e-mails ou sites, diminuindo assim a possibilidade de acesso acidental ao incidentes envolvendo conteúdo de phishing.

Análise da Ocorrência

Visão dos profissionais de GESTIC da CSSBC:

Itens entregues pelo Colaborador de Compras e Contratos:

Recebemos em nossas mãos referidos arquivos abaixo, enviados pelo representante do remetente original (Eduardo Reis [redacted]) sobre o e-mail do dia 14/07/2023 sendo seu remetente [redacted]

Sendo seu conteúdo:

Corpo do e-mail de (Eduardo Reis [redacted]) : Anexo I

Impressão do primeiro e-mail enviado de ([redacted]): Anexo II

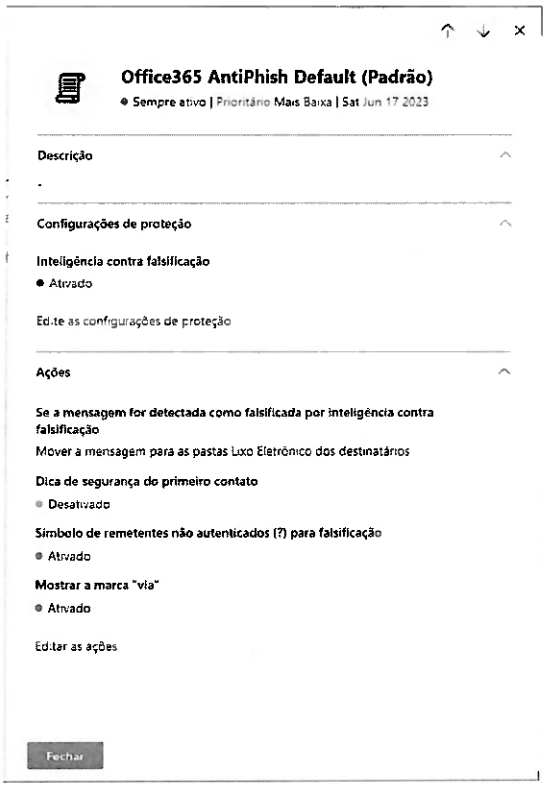
Impressão do segundo e-mail enviado de ([redacted]): Anexo III

Comprovação de entrega do e-mail enviado em Anexo IV

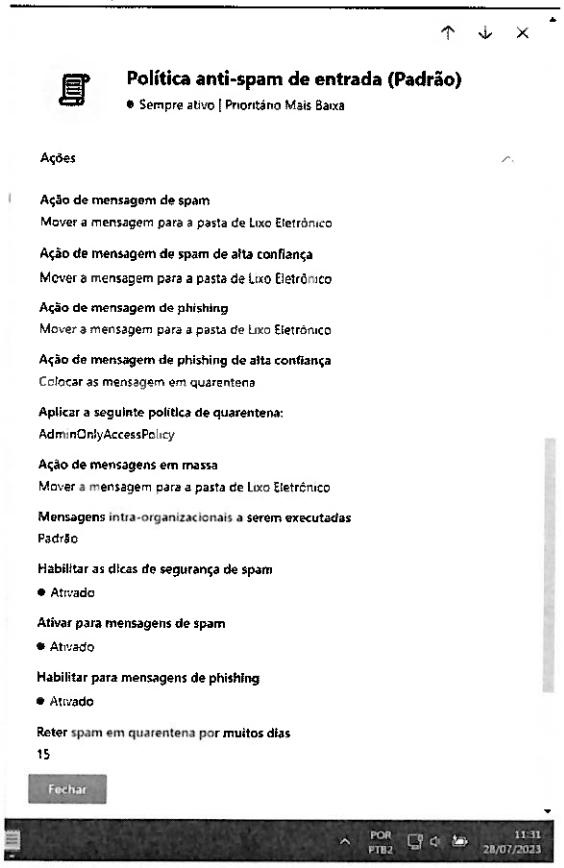
Configuração de Proteções Microsoft:

Como é comum no ambiente de Tecnologia da Informação, as configurações, parametrizações e tecnologias empregadas em um sistema, sempre passarão por um processo de melhoria contínua. Sendo assim, podemos assumir que até a data de 28/07/2023, nosso ambiente apresenta as seguintes políticas habilitadas:

Anti-phishing (Padrão):



Política anti-spam de entrada (Padrão)



Política anti-spam de entrada (Padrão)

● Sempre ativo | Prioritário Mais Baixa

Ações

Ação de mensagem de spam
Mover a mensagem para a pasta de Lixo Eletrônico

Ação de mensagem de spam de alta confiança
Mover a mensagem para a pasta de Lixo Eletrônico

Ação de mensagem de phishing
Mover a mensagem para a pasta de Lixo Eletrônico

Ação de mensagem de phishing de alta confiança
Colocar as mensagem em quarentena

Aplicar a seguinte política de quarentena:
AdminOnlyAccessPolicy

Ação de mensagens em massa
Mover a mensagem para a pasta de Lixo Eletrônico

Mensagens intra-organizacionais a serem executadas
Padrão

Habilitar as dicas de segurança de spam
● Ativado

Ativar para mensagens de spam
● Ativado

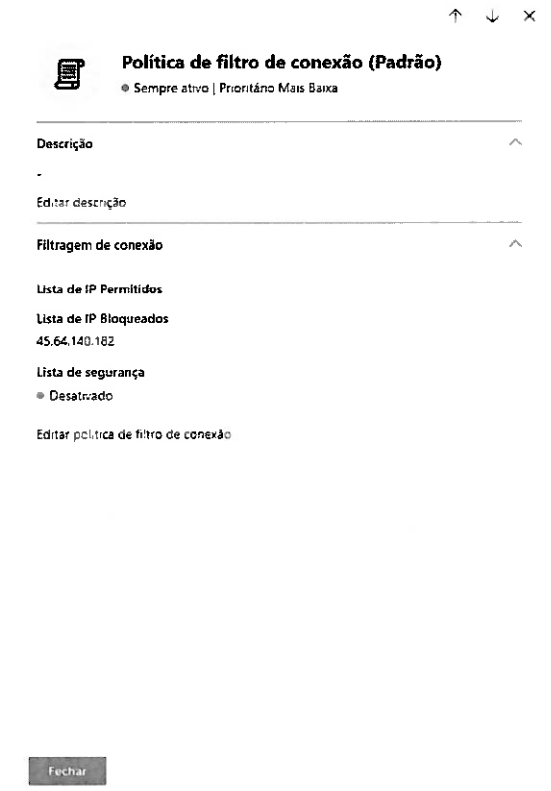
Habilitar para mensagens de phishing
● Ativado

Reter spam em quarentena por muitos dias
15

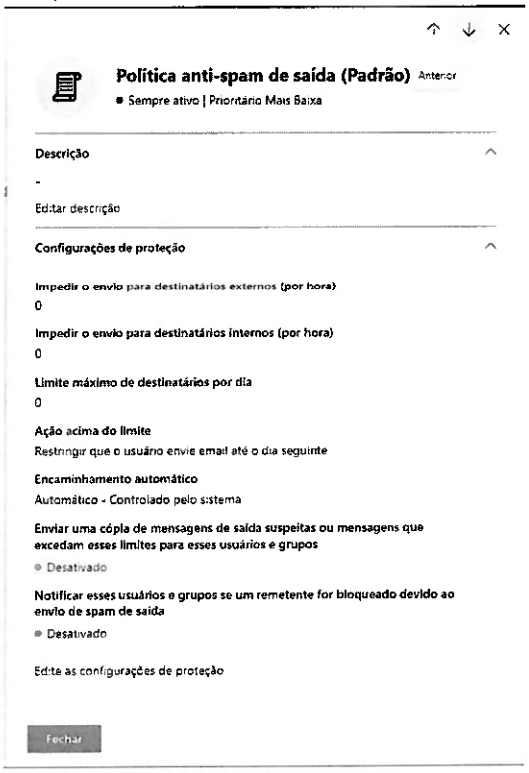
Fechar

POR PTB2 11:31 28/07/2023

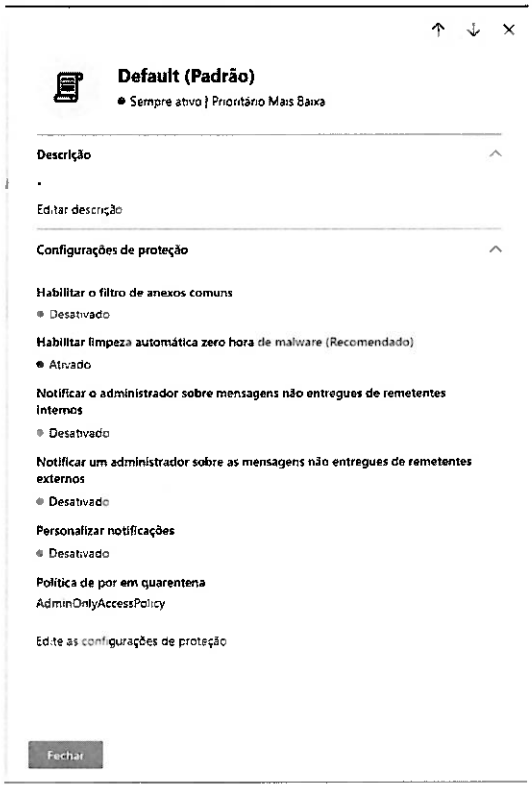
Política de filtro de conexão (Padrão)



Política anti-spam de saída (Padrão)



Política Antimalware (Padrão)



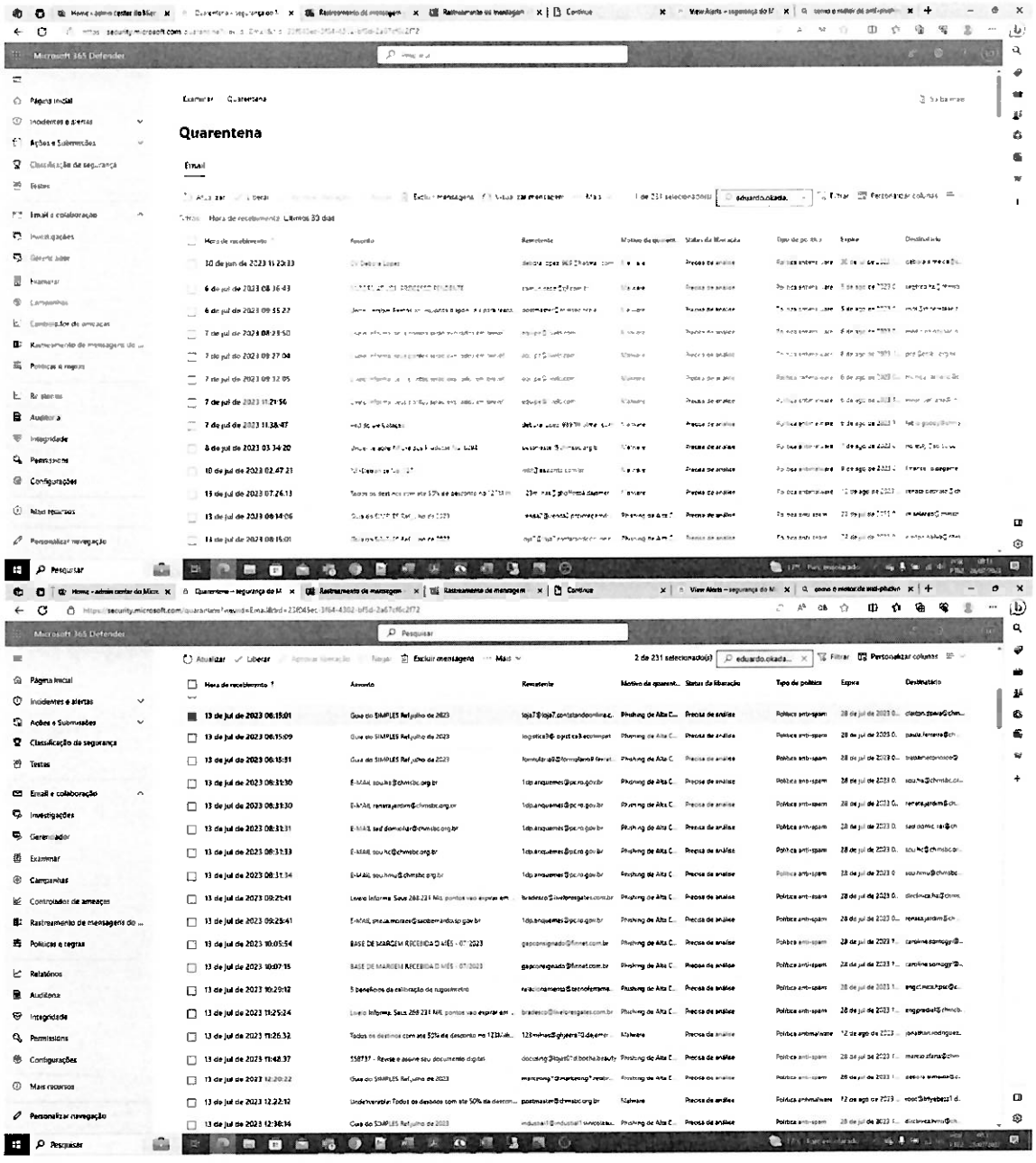
Log:

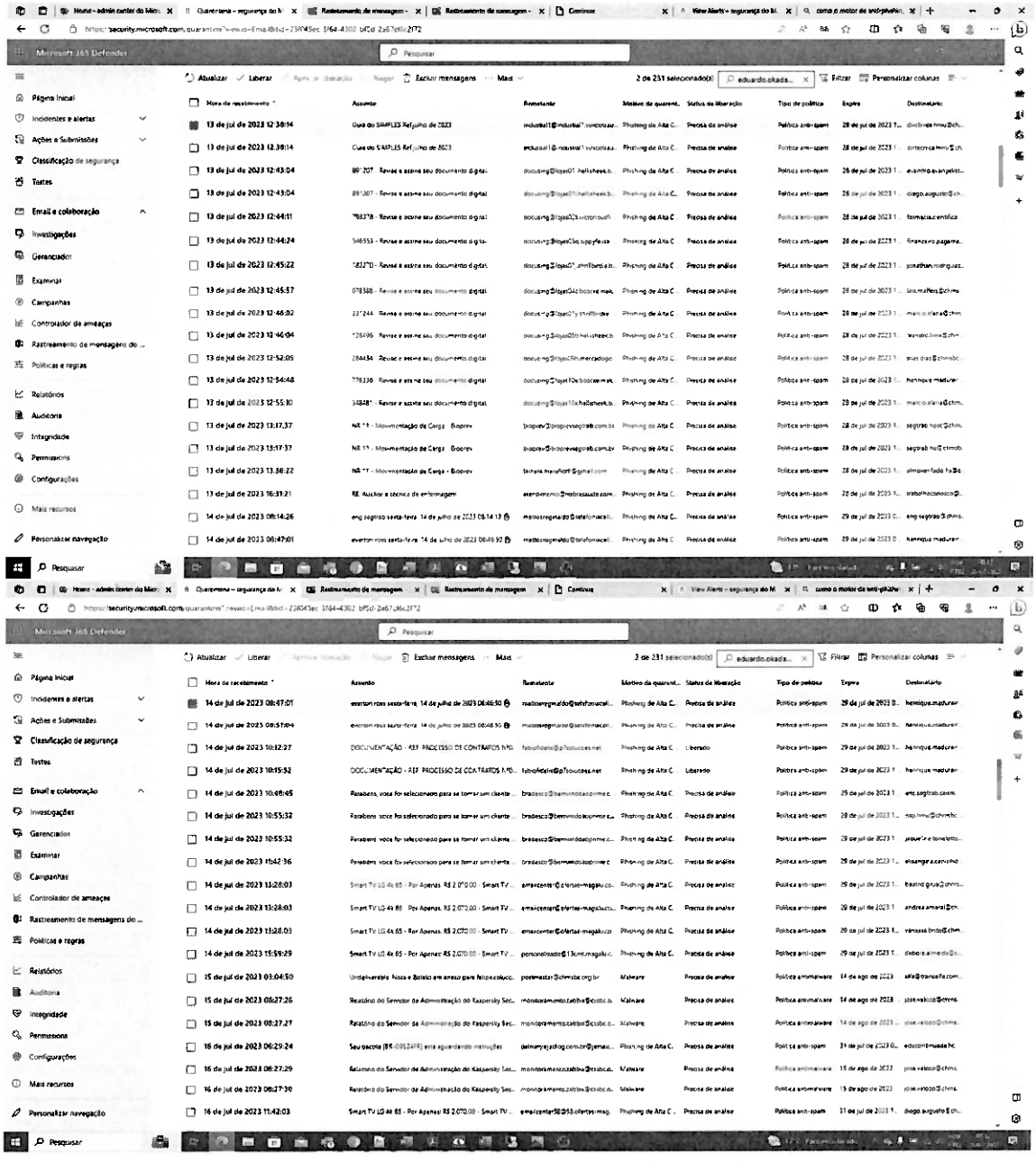
Logs da Caixa de Quarentena total:

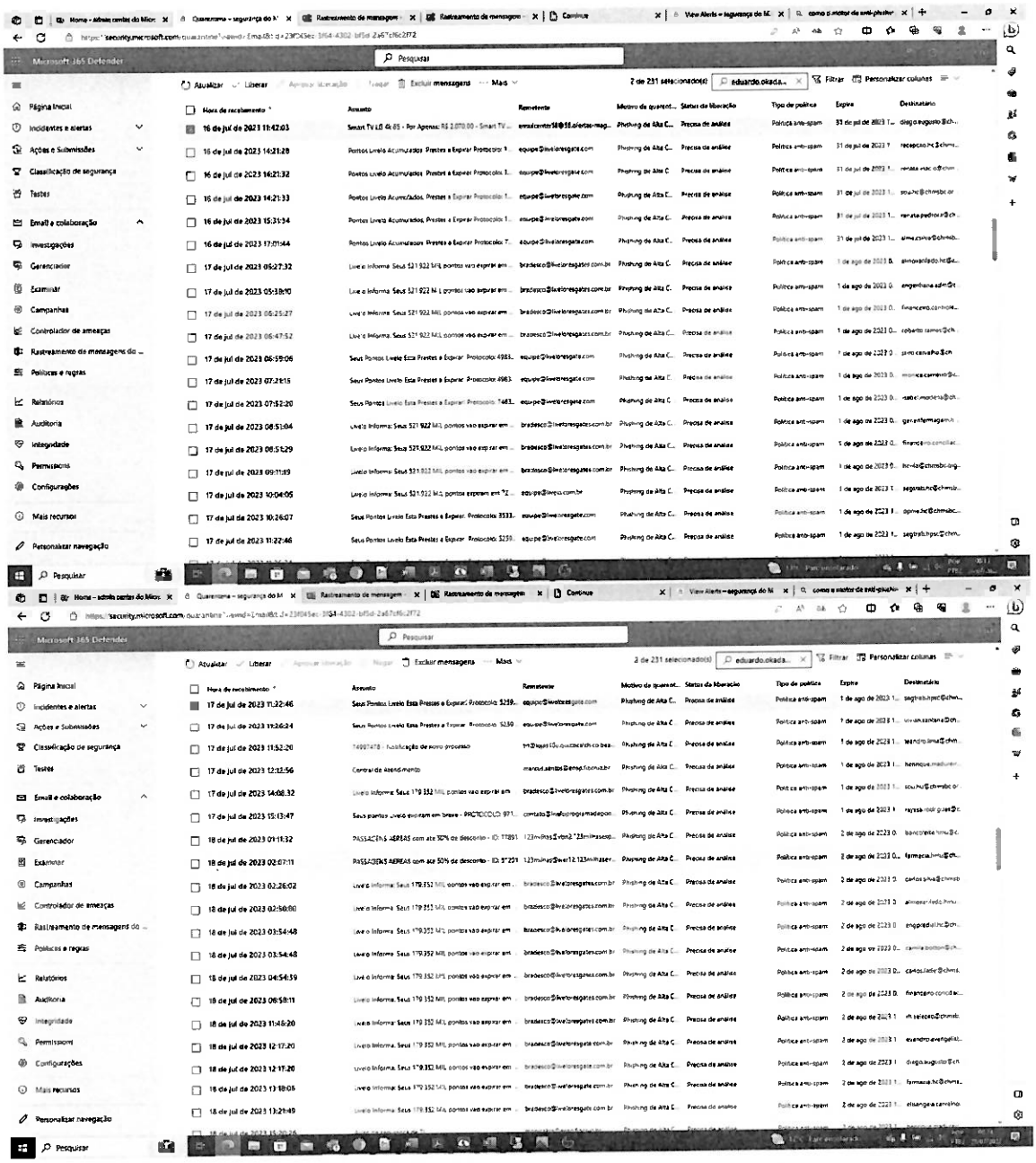
Por apresentar-se extenso e maior que 30 dias não foi possível extrair todo o conteúdo contido na caixa de quarentena, sendo necessário gravar um vídeo de comprovação das inúmeras relações de contidas nessa caixa.

Logs_Quarentena.mp4

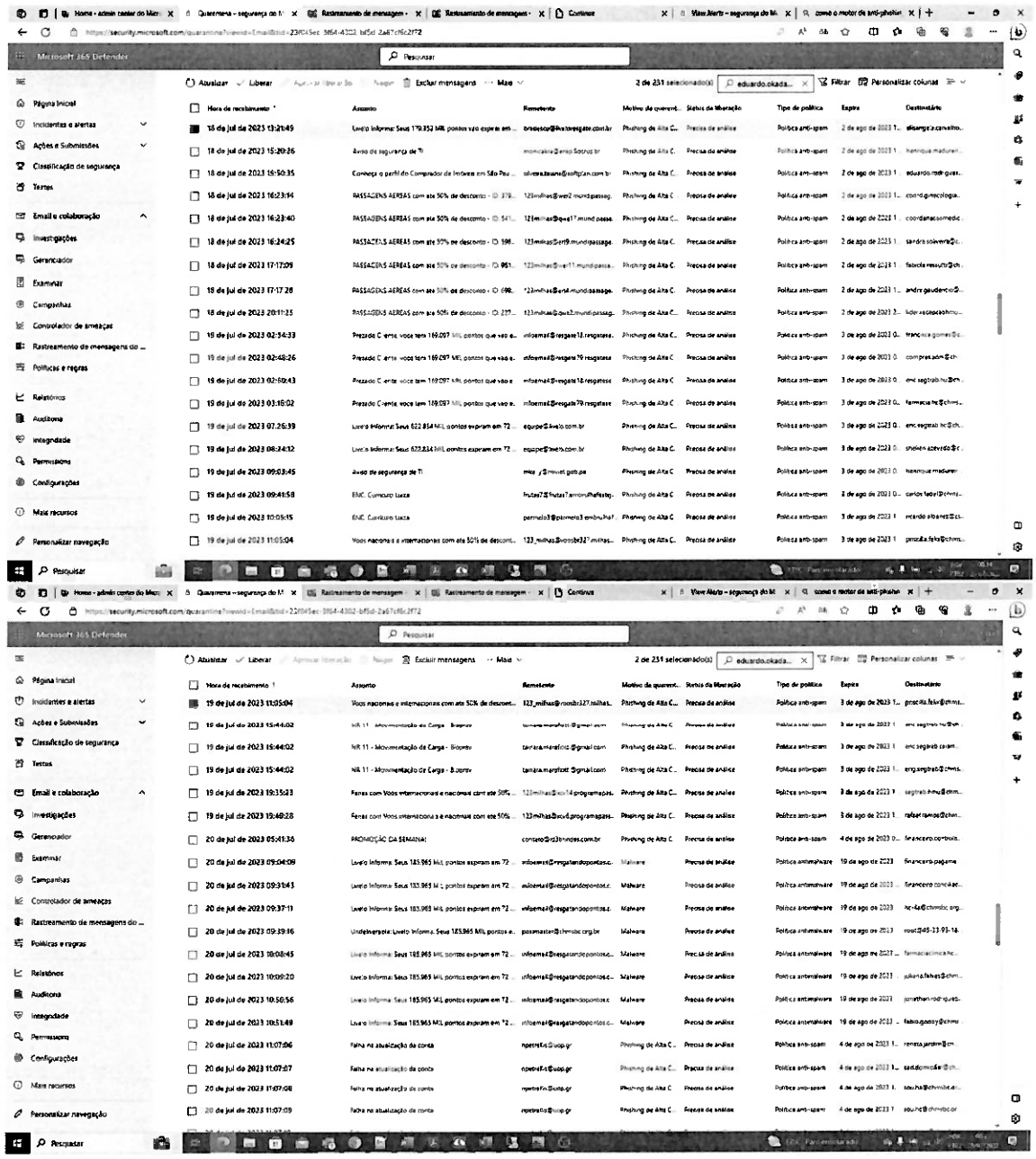
Seguem prints dos itens:


Quarentena
Email
Microsoft 365 Defender
Página inicial
Incidentes e alertas
Ações e Submissões
Classificação de segurança
Testes
Email e colaboração
Investigações
Gerenciador
Examinar
Campanhas
Controladores de ameaças
Rastreamento de mensagens do ...
Políticas e regras
Relatórios
Auditoria
Integridade
Permissões
Configurações
Mais recursos
Personalizar navegação
Pesquisar

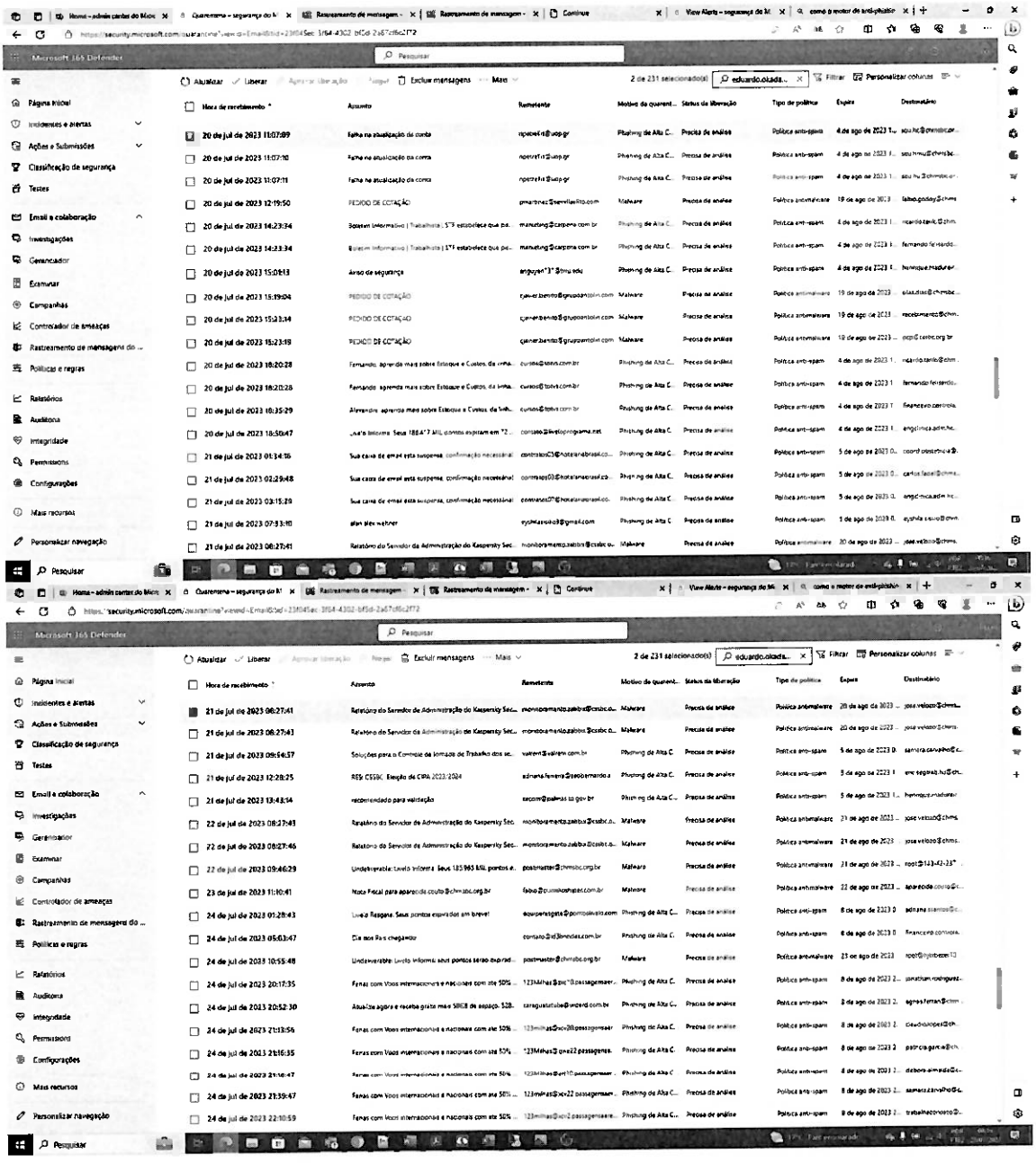




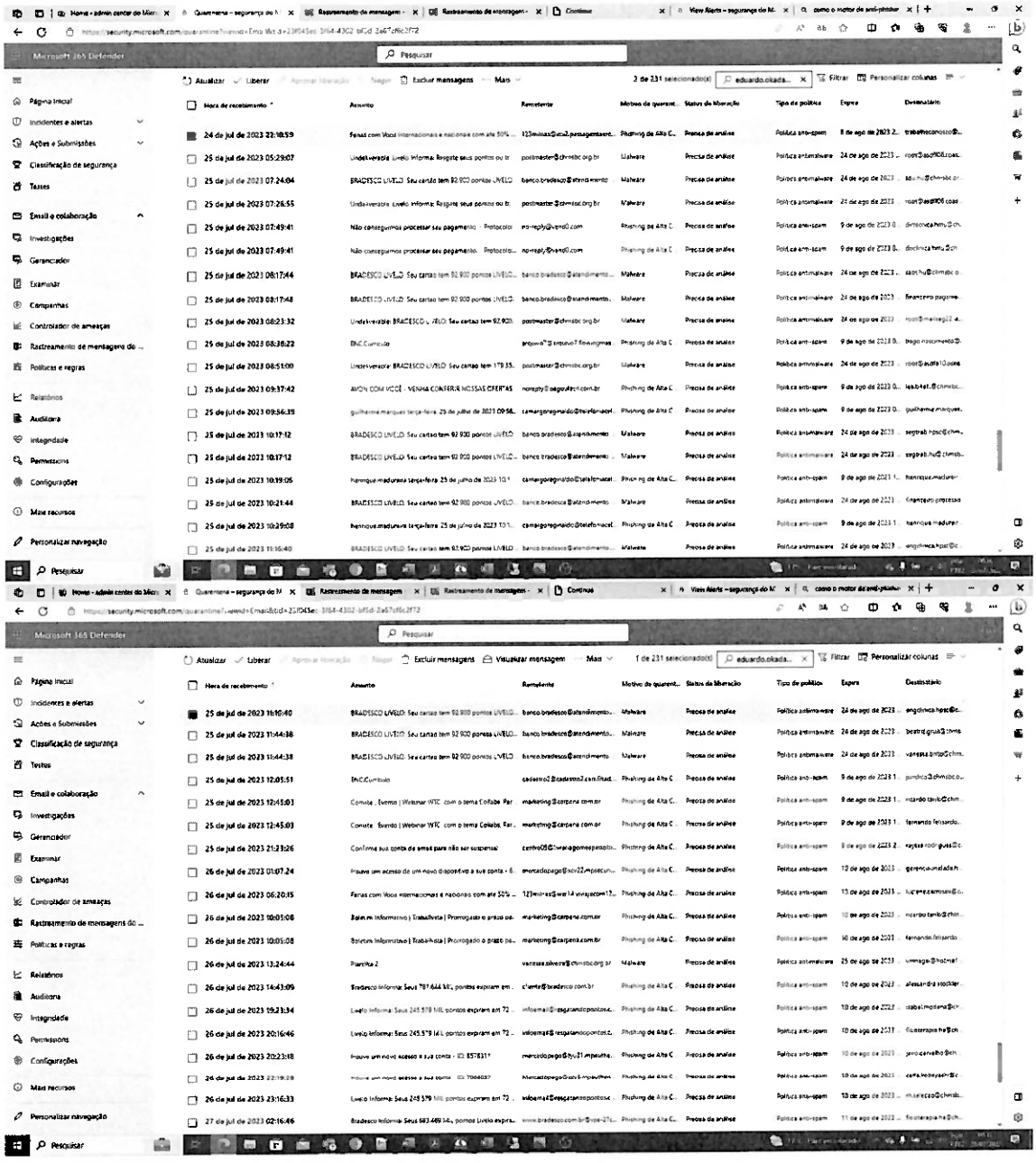
PROC. Nº
FLS 163
VISTO



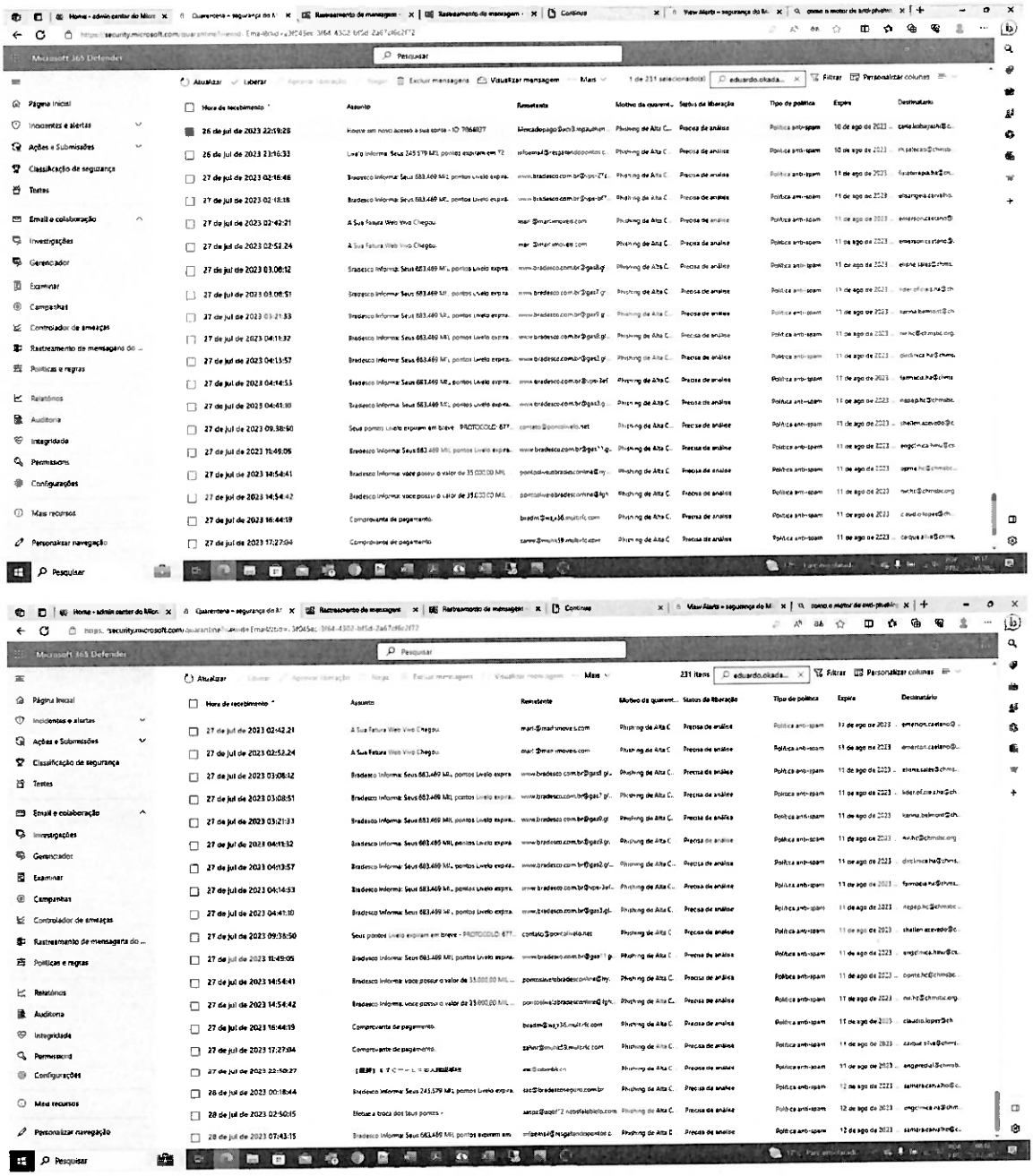
FUNDAÇÃO DO ABC


Microsoft 365 Defender
Pesquisar
Página inicial
Incidentes e alertas
Ações e Submissões
Classificação de segurança
Testes
Email e colaboração
Investigações
Gerenciador
Examinar
Campanhas
Controlador de ameaças
Rastreamento de mensagens do ...
Políticas e regras
Relatórios
Auditoria
Integridade
Permissões
Configurações
Mais recursos
Personalizar navegação
Atualizar
Liberar
Excluir mensagens
Mais
2 de 231 selecionado(s)
eduardo.olaida...
Filtrar
Personalizar colunas
Hora de recebimento
Assunto
Remetente
Motivo da quarent...
Status da liberação
Tipo de política
Expira
Destinatário
20 de jul de 2023 11:07:09
Falha na atualização da conta
20 de jul de 2023 11:07:10
Falha na atualização da conta
20 de jul de 2023 11:07:11
Falha na atualização da conta
20 de jul de 2023 12:19:50
PEDIDO DE COTAÇÃO
20 de jul de 2023 14:23:34
Boletim Informativo | Trabalhista | STF estabelece que pa...
20 de jul de 2023 14:23:34
Boletim Informativo | Trabalhista | STF estabelece que pe...
20 de jul de 2023 15:01:13
Aviso de segurança
20 de jul de 2023 15:19:04
PEDIDO DE COTAÇÃO
20 de jul de 2023 15:23:14
PEDIDO DE COTAÇÃO
20 de jul de 2023 15:23:19
PEDIDO DE COTAÇÃO
20 de jul de 2023 18:20:28
Fernando, aprenda mais sobre Estoque e Custos, da linha...
20 de jul de 2023 18:20:28
Fernando, aprenda mais sobre Estoque e Custos, da linha...
20 de jul de 2023 18:35:29
Alexandre, aprenda mais sobre Estoque e Custos, da linh...
20 de jul de 2023 18:50:47
Você Informa: Seus 188.477 MIL pontos expiram em 72...
21 de jul de 2023 01:14:16
Sua caixa de email está suspensa, confirmação necessária!
21 de jul de 2023 02:29:48
Sua caixa de email está suspensa, confirmação necessária!
21 de jul de 2023 03:15:29
Sua caixa de email está suspensa, confirmação necessária!
21 de jul de 2023 07:53:10
alan alex wehner
21 de jul de 2023 08:27:41
Relatório do Servidor da Administração do Kaspersky Sec...
Pesquisar

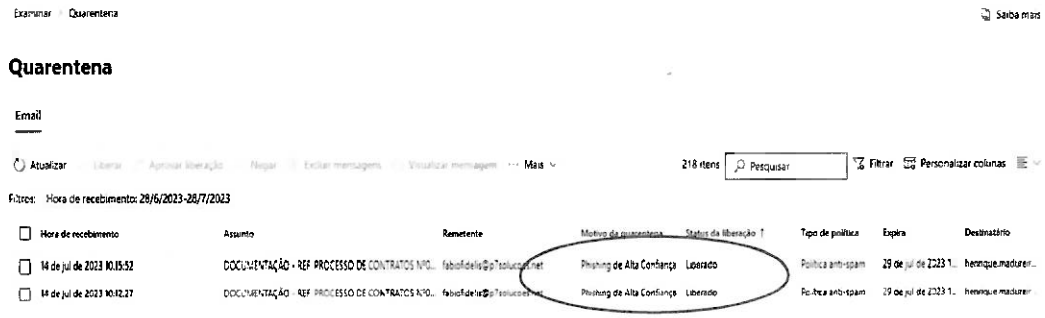
FLS 171



FUNDAÇÃO DO ABC



Assim, evidenciamos que os citados e-mails realmente encontram-se na caixa de quarentena, classificado como phishing de alta confiança, como demonstra a imagem abaixo:



Estatística de eficiência da ferramenta de anti-phishing

Na amostragem de 30 dias, o total é de 216 phishings totais e 4 phishings falso positivos, interpretados de forma humana. Assim, a porcentagem entre phishing reais e falso positivos pode ser transcrita na fórmula abaixo:

phishings e malwares reais = PMR

phishings e malwares totais = PMT

phishings e malwares falso positivos = PMFP

(PMR)= (((PMT) – (PMFP)) /(PMT))*100

Nesta proporção podemos dizer que:

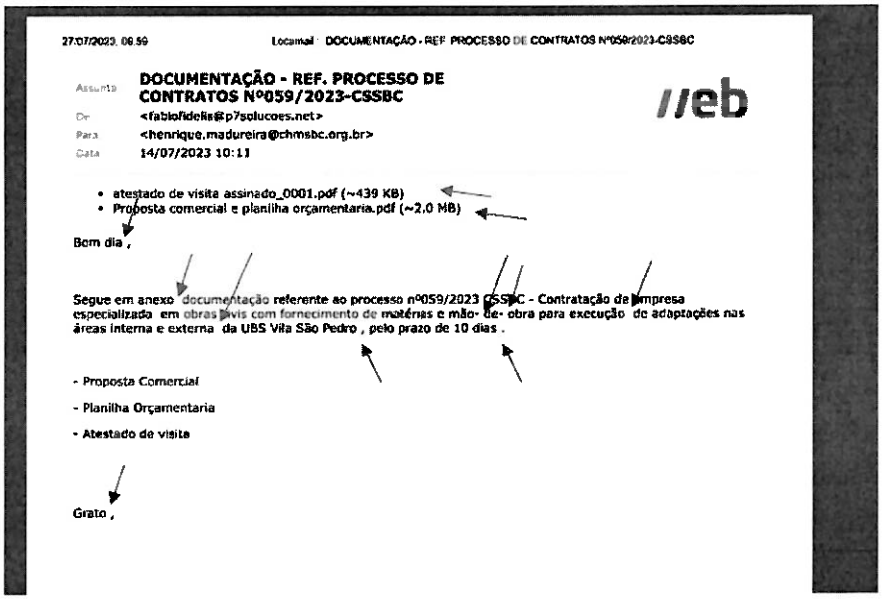
PMA=(216-4)/216*100

PMA=98,14% de efetividade no aprendizado da ferramenta, ou 1,85% de situações falso positivas.

Sobre os e-mails recebidos:

Nossa interpretação sobre o e-mail recebido pelos servidores é de que a classificação do e-mail como um phishing de alta confiança pode ter se originado por 3 situações cruzadas: conter anexos, título corporativo, porém composição textual com divergências ortográficas, como sugere o documento da Microsoft (referência: https://support.microsoft.com/pt-br/windows/proteja-se-contra-phishing-0c7ea947-ba98-3ade-7214-430e11860a44)

- **Ortografia e gramática ruim** – empresas e organizações profissionais geralmente têm uma equipe editorial para garantir que os clientes obtenham conteúdo profissional e de alta qualidade. Se uma mensagem de email apresentar erros ortográficos ou gramaticais óbvios, pode ser um golpe. Às vezes, esses erros são o resultado de uma tradução inadequada de um idioma estrangeiro e, às vezes, são deliberados na tentativa de escapar dos filtros que tentam bloquear esses ataques.



27/07/2023, 08:59 Locamail - DOCUMENTAÇÃO - REF. PROCESSO DE CONTRATOS Nº059/2023-CSSBC

Assunto: **DOCUMENTAÇÃO - REF. PROCESSO DE CONTRATOS Nº059/2023-CSSBC**

De: <fabiofideles@p7solucoes.net>

Para: <henrique.madureira@chmsbc.org.br>

Data: 14/07/2023 10:11

- atestado de visita assinado_0001.pdf (~439 KB)
- Proposta comercial e planilha orçamentaria.pdf (~2,0 MB)

Bom dia ,

Segue em anexo documentação referente ao processo nº059/2023 CSSBC - Contratação de empresa especializada em obras civis com fornecimento de matérias e mão- de- obra para execução de adaptações nas áreas interna e externa da UBS Vila São Pedro , pelo prazo de 10 dias .

- Proposta Comercial
- Planilha Orçamentaria
- Atestado de visita

Grato ,

As setas em vermelho destacam os anexos, acrescidos dos erros relatados. Como podemos ver, o título do e-mail é uma proposta corporativa, acrescida de anexos, porém, o corpo do e-mail apresenta algumas incoerências, como espaços antes das vírgulas, duplo espaços entre as palavras e a palavra mão-de-obra com espaços ao final de cada hífen (ex: mão- de- obra).

Assim, em nosso entendimento, poderia a ferramenta entender que se trata de possível phishing de alto grau de coerência, podendo ser considerado um risco de falsa informação.

Verificando isso, a regra padrão do anti-spam e anti-phishing e acrescido da análise da baixa taxa de falso positivo, concluímos que sem uma solicitação formal direta do colaborador, esse e-mail só seria detectado e liberado no começo do mês de forma manual, quando ocorre a revisão periódica da quarentena e ainda a depender da interpretação do administrador do Microsoft 365, não havendo forma automática para liberação do mesmo, nas configurações padrões da Microsoft, aplicada em nosso servidor de e-mail.

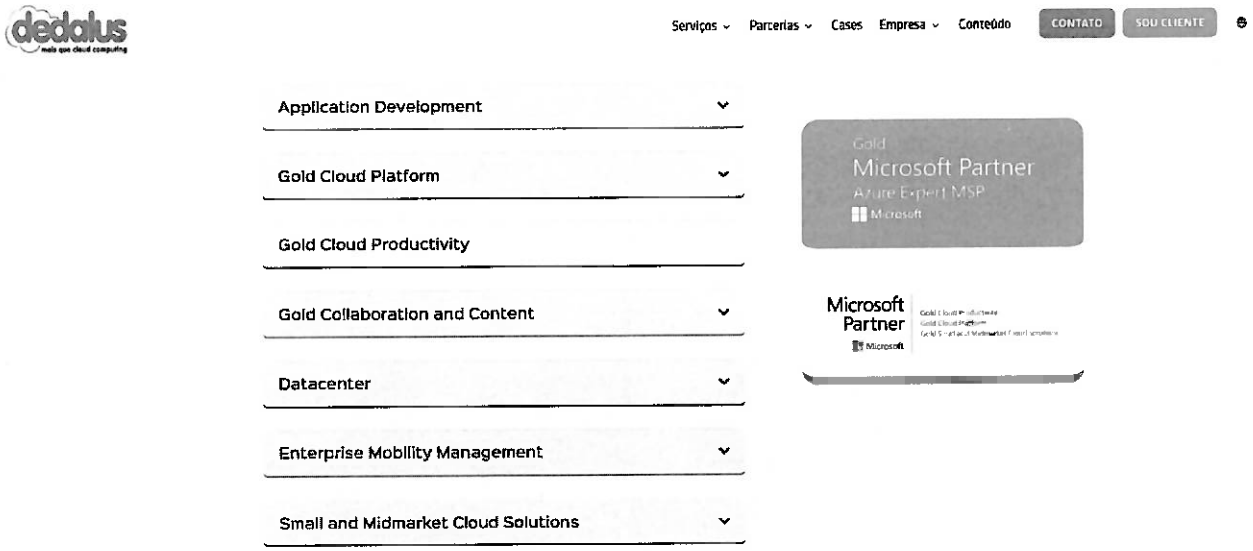
> ⓘ **Observação**
>
> Os usuários não podem liberar suas próprias mensagens que foram colocadas em quarentena como malware por políticas anti-malware ou Anexos Seguros, ou como phishing de alta confiança por políticas anti-spam, independentemente de como a política de quarentena está configurada. Se a política permitir que os usuários liberem suas próprias mensagens em quarentena, os usuários poderão *solicitar* a liberação de seu malware em quarentena ou mensagens de phishing de alta confiança.

( )

Assim, é importante frisarmos que a ferramenta tem um alto grau de confiabilidade e baixa taxa de erro ou desvio padrão, reduzindo de forma considerável, porém imensurável o impacto que poderia ser encontrado no caso de sua desativação.

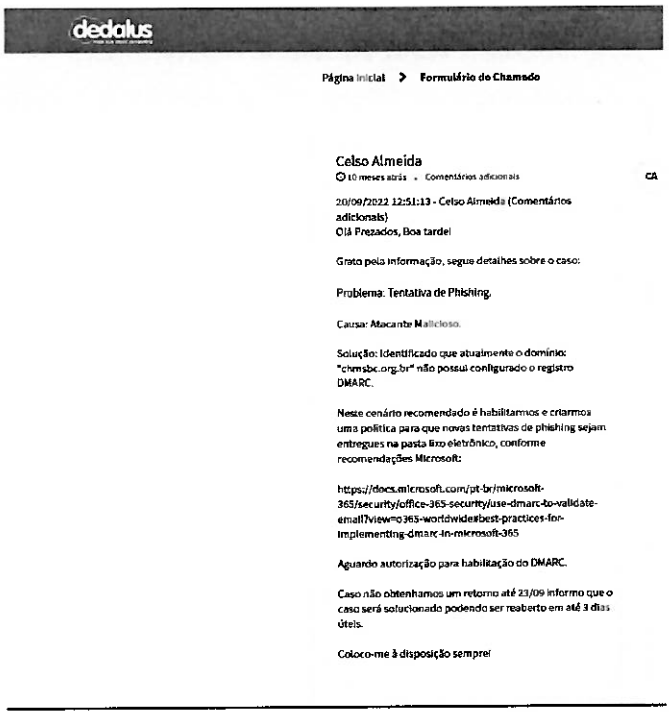
Empresa mantenedora de nosso ambiente "Microsoft 365":

Dedalus Prime empresa certificada Microsoft que nos fornece a plataforma. Conta com um gigantesco número de projetos comercializados e implementados, dos mais variados tamanhos, de Office 365 e Microsoft 365, o que dá ao time a expertise necessária para oferecer ao cliente sempre o melhor cenário, otimizando suas jornadas de transformação digital.



Visão equipe tecnologia da informação CSSBC sobre a ferramenta:

Diversas tentativas de phishing foram relatadas a partir setembro de 2022. Temendo uma situação irreversível e risco materializado, em análise conjunta com o suporte da empresa Dedalus, implementamos dentro do nosso ambiente, politicas anti-phishing e uma regra de entrega como demonstrado abaixo:


dedalus

Página inicial > Formulário do Chamado

Celso Almeida
10 meses atrás . Comentários adicionais CA

20/09/2022 12:51:13 - Celso Almeida (Comentários adicionais)
Olá Prezados, Boa tarde!

Grato pela informação, segue detalhes sobre o caso:

Problema: Tentativa de Phishing.

Causa: Atacante Malicioso.

Solução: Identificado que atualmente o domínio "chmsbc.org.br" não possui configurado o registro DMARC.

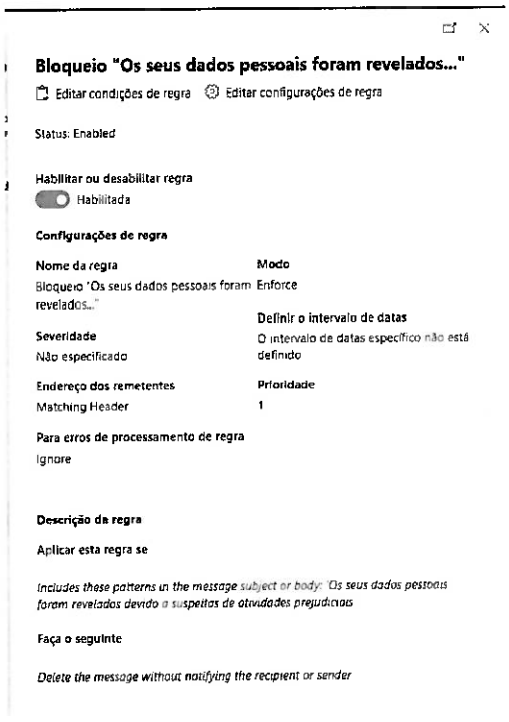
Neste cenário recomendado é habilitarmos e criarmos uma política para que novas tentativas de phishing sejam entregues na pasta lixo eletrônico, conforme recomendações Microsoft:

https://docs.microsoft.com/pt-br/microsoft-365/security/office-365-security/use-dmarc-to-validate-email?view=o365-worldwide#best-practices-for-implementing-dmarc-in-microsoft-365

Aguardo autorização para habilitação do DMARC.

Caso não obtenhamos um retorno até 23/09 informo que o caso será solucionado podendo ser reaberto em até 3 dias úteis.

Coloco-me à disposição sempre!


Bloqueio "Os seus dados pessoais foram revelados..."

Editar condições de regra Editar configurações de regra

Status: Enabled

Habilitar ou desabilitar regra
Habilitada

Configurações de regra

Nome da regra
Bloqueio "Os seus dados pessoais foram revelados..."

Modo
Enforce

Definir o intervalo de datas
O intervalo de datas específico não está definido

Severidade
Não especificado

Endereço dos remetentes
Matching Header

Prioridade
1

Para erros de processamento de regra
Ignore

Descrição da regra

Aplicar esta regra se

Includes these patterns in the message subject or body: 'Os seus dados pessoais foram revelados devido a suspeitas de atividades prejudiciais

Faça o seguinte

Delete the message without notifying the recipient or sender

Após a aplicação das políticas anti-phishing, reduzimos a quantidade de phishing recebidos diretamente nas caixas de entradas e mantivemos o ambiente seguro, sem ameaças. O caso de falso positivo discorrido neste documento é o primeiro desde a ativação da regra em 2022. Novamente, após análise, verificamos que houve a classificação do e-mail como phishing, uma possível correta pontuação, assim validando o funcionamento da aplicação e mantendo sua taxa de assertividade alta.

Durante todo o progresso da elaboração deste documento, solicitamos à Dedalus que fizesse suas análises e considerações dos e-mails envolvidos. Suas considerações técnicas, estão contidas no capítulo a seguir.

Visão profissionais Dedalus:

Segundo a Dedalus empresa mantenedora de nosso ambiente "Microsoft 365":

"Analisando o cabeçalho da mensagem é possível verificar que a mensagem entrou com pontuação SCL 8, o que indica alta possibilidade de ser spam/phishing. Essa pontuação é alterada de acordo com as análises feitas pelo Exchange Online Protection e pelas configurações do antispam e, quanto maior a pontuação, maior a probabilidade de ser um spam/phishing.

As análises incluem inúmeras variáveis, por exemplo, reputação do domínio de origem, reputação do IP de origem, autenticação e autorização das mensagens de e-mail do domínio de origem, entre muitos outros. No cabeçalho da mensagem existem as informações a respeito da classificação, porém, não são informações publicamente acessíveis (item "Spam rules" do cabeçalho), sendo assim, não temos os motivos exatos que levaram à esta classificação, temos apenas a informação que inúmeros itens foram avaliados (na entrada da mensagem) deixando a mensagem com pontuação 8 no SCL, classificando-a como phishing de alta confiança e redirecionando a mensagem para a quarentena.

Caso o remetente seja conhecido e confiável, é possível adicionar o domínio do mesmo na whitelist de seu antispam e reportar a mensagem em questão para a Microsoft, indicando que não é um spam/phishing."

Summary

Subject	DOCUMENTAÇÃO - REF. PROCESSO DE CONTRATOS Nº059/2023-CSSBC
Message Id	<54eb77ed489ae222b1cef899097b30db@p7solucoes.net>
Creation time	Fri, 14 Jul 2023 10:15:44 -0300 (Delivered after 9 seconds)
From	fabiofidelis@p7solucoes.net
To	henrique.madureira@chmsbc.org.br

+ Received headers

Forefront Antispam Report Header

Country/Region	BR
Language	pt
Spam Confidence Level	8
Spam Filtering Verdict	SPM
IP Filter Verdict	NLI
HELO/EHLO String	mail4953.hm1315.locaweb.com.br
PTR Record	mail4953.hm1315.locaweb.com.br
Connecting IP Address	201.76.49.53
Protection Policy Category	HPHISH
Spam rules	(13230028)(451199021)(1096003)(22186003)(6966003)(6916009)(28085005)(5660300002)(58800400005)(108616005)(33964004)(24736004)(356005)(86362001)(26005)(9686003)(7636003)(224303003)(6266002)(21480400003)(336012)(36756003)(7596003)(2616005)(7126003)(43356004)
Source header	CIP:201.76.49.53;CTRY:BR;LANG:pt;SCL:8;SRV:;IPV:NLI;SFV:SPM;H:mail4953.hm1315.locaweb.com.br;PTR:mail4953.hm1315.locaweb.com.br;CAT:HPHISH;SFS:(13230028)(451199021)(1096003)(22186003)(6966003)(6916009)(28085005)(5660300002)(58800400005)(108616005)(33964004)(24736004)(356005)(86362001)(26005)(9686003)(7636003)(224303003)(6266002)(21480400003)(336012)(36756003)(7596003)(2616005)(7126003)(43356004);DIR:INB;
Unknown fields	DIR:INB;

Microsoft Antispam Header

Bulk Complaint Level	0
Source header	BCL:0

Conclusão

Através do texto preposto e das análises realizadas, concluímos que o evento relacionado ocorreu pelo bloqueio através da ferramenta anti-phishing da Microsoft, motivado pelas características da mensagem enviada pelo remetente e recebido pelo servidor de e-mail, não havendo manipulação manual nas considerações realizadas pela ferramenta. A hipótese mais provável da classificação é a apresentada pela GESTIC do CSSBC, motivada pela composição dos fatores de formatação de texto da mensagem, sua importância e anexos, acrescido das considerações realizadas pela Dedalus, que motivou que a ferramenta classificasse a mensagem como "phishisng de alta confiança". Concluindo, não havendo atuação possível nas configurações padrões e dentro do prazo mencionado como fatal, sem que houvesse uma solicitação por parte do colaborador do CSSBC.

Ainda citamos que a própria Dedalus não discorre sobre todos os itens presentes na inteligência e das regras de negócios adotadas pela tecnologia anti-phishing empregada pela Microsoft, sendo esta protegida por segredos comerciais. Assim, podemos apenas elaborar hipóteses sobre a classificação das mensagens mencionadas.

Em tempo, não recomendamos a desativação da ferramenta de anti-phishing, que contribui de forma positiva na segurança, confiabilidade e integridade das informações neste CSSBC.

Bibliografia

https://support.microsoft.com/pt-br/windows/proteja-se-contra-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

https://br.malwarebytes.com/phishing/

https://learn.microsoft.com/pt-br/microsoft-365/security/office-365-security/anti-phishing-protection-about?view=o365-worldwide

FLS 138

Anexos:

Anexo I:

De: Eduardo Reis <erels.adv@hotmail.com>
Enviado: quinta-feira, 27 de julho de 2023 10:30
Para: fabiofidelis@p7solucoes.net <fabiofidelis@p7solucoes.net>; Henrique Lopes Madureira dos Santos <henrique.madureira@chmsbc.org.br>; Adriana Santana Santos <adriana.ssantos@chmsbc.org.br>
Assunto: RE: DOCUMENTAÇÃO - REF. PROCESSO DE CONTRATOS Nº059/2023-CSSBC

Prezado Henrique Madureira, bom dia.

Sou o Dr. Eduardo, advogado da empresa P7 Soluções. Me apresento.

Ab initio, sirvo-me deste para encaminhar, em anexo, digitalização de 2 (dois) e-mails, ambos datados e enviados no dia 14/07/2023 a confirmação de envio às 10H11min e 10H15min, respectivamente.

Igual forma, encaminhamos em anexo o comprovante de envio dos referidos documentos (DOC. 03).

Constam, ainda, como anexos destes:

- Atestado de visitas devidamente assinado;
- Proposta Comercial e planilha orçamentária.

Conforme se observa, os e-mails foram enviados/respondidos à henrique.madureira@chmsbc.org.br, de titularidade de Vossa Senhoria, em tempo hábil ao seu recebimento.

Neste sentido, para evitarmos judicialização da presente licitação, solicitamos e reiteramos, respeitosamente, à Vossa Senhoria, esclarecimentos sobre a recusa da proposta enviada, considerando a proposta e orçamento proposto por P7 Soluções, eis que comprovado o efetivo envio da documentação necessária.

Desde já agradeço a atenção dispensada por Vossa Senhoria.

Permanecemos à disposição.

Atenciosamente,

Eduardo Gomes dos Reis

FLS 137

Anexo II:

Assunto: **DOCUMENTAÇÃO - REF. PROCESSO DE CONTRATOS Nº059/2023-CSSBC**

De <fablofidelis@p7solucoes.net>

Para: <henrique.madureira@chmsbc.org.br>

Data 14/07/2023 10:11

- atestado de visita assinado_0001.pdf (~439 KB)
- Proposta comercial e planilha orçamentaria.pdf (~2.0 MB)

Bom dia ,

Segue em anexo documentação referente ao processo nº059/2023 CSSBC - Contratação de empresa especializada em obras civis com fornecimento de matérias e mão- de- obra para execução de adaptações nas áreas interna e externa da UBS Vila São Pedro , pelo prazo de 10 dias .

- Proposta Comercial
- Planilha Orçamentaria
- Atestado de visita

Grato ,

FLS 180

Anexo III:

Assunto: **DOCUMENTAÇÃO - REF. PROCESSO DE CONTRATOS Nº059/2023-CSSBC**

De <fabiofidelis@p7solucoes.net>

Para: <henrique.madureira@chmsbc.org.br>

Data 14/07/2023 10:15

- atestado de visita assinado_0001.pdf (~439 KB)
- Proposta comercial e planilha orçamentaria.pdf (~2.0 MB)

Bom dia ,

Segue em anexo documentação referente ao processo nº059/2023 CSSBC - Contratação de empresa especializada em obras civis com fornecimento de matérias e mão- de- obra para execução de adaptações nas áreas interna e externa da UBS Vila São Pedro , pelo prazo de 10 dias .

- Proposta Comercial
- Planilha Orçamentaria
- Atestado de visita

Grato ,

Anexo IV

Assunto **Delivered: DOCUMENTAÇÃO - REF. PROCESSO DE CONTRATOS Nº059/2023-CSSBC**
De <postmaster@chmsbc.org.br>
Para <fabiofidelis@p7solucoes.net>
Data 14/07/2023 10:15

//eb

Your message has been delivered to the following recipients:

henrique.madureira@chmsbc.org.br

Subject: DOCUMENTAÇÃO - REF. PROCESSO DE CONTRATOS Nº059/2023-CSSBC


```
Reporting-MTA: dns;CPWP152MB5144.LAMP152.PROD.OUTLOOK.COM
Received-From-MTA: dns;mail4953.hm1315.locaweb.com.br
Arrival-Date: Fri, 14 Jul 2023 13:15:53 +0000

Original-Recipient: rfc822;henrique.madureira@chmsbc.org.br
Final-Recipient: rfc822;henrique.madureira@chmsbc.org.br
Action: delivered
Status: 2.0.0
Diagnostic-Code: smtp;250 2.0.0 OK
```

```
Content-Type: multipart/mixed;
    boundary="_37e0661d-f917-4f43-bec0-5e354cc0b701_"
X-MS-Exchange-Organization-InternalOrgSender: False
Received: from DM6PR06CA0005.namprd06.prod.outlook.com (2603:10b6:5:120::18)
 by CPWP152MB5144.LAMP152.PROD.OUTLOOK.COM (2603:10d6:103:15e::13) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6588.27; Fri, 14 Jul
 2023 13:15:53 +0000
Received: from DM3NAM02FT021.eop-nam02.prod.protection.outlook.com
 (2603:10b6:5:120:cafe::47) by DM6PR06CA0005.outlook.office365.com
 (2603:10b6:5:120::18) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6588.27 via Frontend
 Transport; Fri, 14 Jul 2023 13:15:52 +0000
Authentication-Results: spf=pass (sender IP is 201.76.49.53)
 smtp.mailfrom=p7solucoes.net; dkim=none (message not signed)
 header.d=none;dmarc=bestguesspass action=none
 header.from=p7solucoes.net;compauth=pass reason=109
Received-SPF: Pass (protection.outlook.com: domain of p7solucoes.net
 designates 201.76.49.53 as permitted sender) receiver=protection.outlook.com;
 client-ip=201.76.49.53; helo=mail4953.hm1315.locaweb.com.br; pr=C
Received: from mail4953.hm1315.locaweb.com.br (201.76.49.53) by
 DM3NAM02FT021.mail.protection.outlook.com (10.13.4.249) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.6588.24 via Frontend Transport; Fri, 14 Jul 2023 13:15:51 +0000
Received: from mcbain0008.email.locaweb.com.br (189.126.112.84) by mail4950.hm1315.locaweb.com.br id he55842n8lgj for <henrique.madureira@chmsbc.org.br>; Fri,
14 Jul 2023 10:15:45 -0300 (envelope-from <fabiofidelis@p7solucoes.net>)
X-Original-To: <henrique.madureira@chmsbc.org.br>
Received: from mcbain0008.email.locaweb.com.br (localhost [127.0.0.1])
    by mcbain0008.email.locaweb.com.br (Postfix) with ESMTP id EDECE40D80
    for <henrique.madureira@chmsbc.org.br>; Fri, 14 Jul 2023 10:09:23 -0300 (-03)
Received: from dragonite0020.email.locaweb.com.br (dragonite0020.email.locaweb.com.br [10.31.120.127])
    by mcbain0008.email.locaweb.com.br (Postfix) with ESMTP id A208140078
    for <henrique.madureira@chmsbc.org.br>; Fri, 14 Jul 2023 10:09:20 -0300 (-03)
X-locaweb-id: kCvAz2lF7t1I59PG5EnAD4-
0ithAQz0tnulsQ4igQ1r7S2Xmj3NSSvrs2phoF2RrGJXxTgJLqBJynSG8ayHwtAjIRuQ5yjR_eCI18ODGJSyVQsoxToaV2ov3TiupWpN0M8sbGWQKKugTLwqSPAOWM9VEVXQeFCIyTH1c507xzz_RVewI_o0fmnW
NjY2MTVyNjk2ZjY2Njk2NDY1NmM2OTczNDA3MDM3NzM2ZjZjNzU2MzZmNjU3MzIlNmU2NTc0
Received: from webmail-seguro.com.br (localhost [127.0.0.1])
    (Authenticated sender: fabiofidelis@p7solucoes.net)
    by dragonite0020.email.locaweb.com.br (Postfix) with ESMTPA id E2F101635C7
    for <henrique.madureira@chmsbc.org.br>; Fri, 14 Jul 2023 10:15:44 -0300 (-03)
MIME-Version: 1.0
Date: Fri, 14 Jul 2023 10:15:44 -0300
From: fabiofidelis@p7solucoes.net
To: henrique.madureira@chmsbc.org.br
Subject: =?UTF-8?Q?DOCUMENTA=C3=87=C3=83O_-_REF=2E_PROCESSO_DE_CONTRATOS_?=
 =?UTF-8?Q?N=C2=BA059/2023-CSSBC?=
In-Reply-To: <ae3f001fe07511dc9c19e389db07d210@p7solucoes.net>
References: <ae3f001fe07511dc9c19e389db07d210@p7solucoes.net>
Return-Receipt-To: fabiofidelis@p7solucoes.net
Disposition-Notification-To: fabiofidelis@p7solucoes.net
Message-ID: <54eb77ed489ae222b1cef899097b30db@p7solucoes.net>
X-Sender: fabiofidelis@p7solucoes.net
User-Agent: Roundcube Webmail/1.4.11
Return-Path: fabiofidelis@p7solucoes.net
X-MS-Exchange-Organization-OriginalArrivalTime: 14 Jul 2023 13:15:51.6537
 (UTC)
X-MS-Exchange-Organization-ExpirationStartTime: 14 Jul 2023 13:15:52.2474
 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000
X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit
X-MS-Exchange-Organization-Network-Message-Id:
 fa5ecd71-3443-4aee-354a-08db846c72ec
X-MS-Exchange-Organization-OriginalClientIPAddress: 201.76.49.53
X-MS-Exchange-Organization-OriginalServerIPAddress: 10.13.4.249
X-EOPAttributedMessage: 0
X-EOPTenantAttributedMessage: 23f045ec-3f64-4302-bf5d-2a67cf6c2f72:0
X-MS-Exchange-Organization-TargetResourceForest: LAMP152.PROD.OUTLOOK.COM
X-MS-Exchange-Organization-OrgEopForest: NAM02
X-MS-Exchange-Organization-MessageDirectionality: Incoming
X-MS-Exchange-Organization-Id: 23f045ec-3f64-4302-bf5d-2a67cf6c2f72
X-MS-Exchange-Organization-FFO-ServiceTag: NAM02B
X-MS-Exchange-Organization-Cross-Premises-Headers-Processed:
 DM3NAM02FT021.eop-nam02.prod.protection.outlook.com
X-MS-Exchange-Organization-ConnectingIP: 201.76.49.53
X-MS-Exchange-Organization-ConnectingEHLO: mail4953.hm1315.locaweb.com.br
X-MS-Exchange-Organization-AS-LastExternalIp: 201.76.49.53
X-MS-Exchange-Organization-Originating-Country: BR
X-MS-Exchange-Organization-OriginalEnvelopeRecipients:
 henrique.madureira@chmsbc.org.br
X-MS-Exchange-Organization-PtrDomains: mail4953.hm1315.locaweb.com.br
X-MS-Exchange-Organization-EhloAndPtrDomain:
 mail4953.hm1315.locaweb.com.br;mail4953.hm1315.locaweb.com.br
X-MS-Exchange-Organization-MxPointsToUs: true
```

```
X-MS-Exchange-Organization-RecipientDomainMxRecord-PFAFD:
 chmsbc.org.br#chmsbc-org-br.mail.protection.outlook.com
X-MS-Exchange-Organization-RecipientDomainMxInfo:
 chmsbc.org.br#Office365#chmsbc-org-br.mail.protection.outlook.com
X-MS-Exchange-Organization-CompAuthRes: pass
X-MS-Exchange-Organization-CompAuthReason: 109
X-MS-Exchange-Organization-SpoofDetection-Frontdoor-DisplayDomainName:
 p7solucoes.net
X-MS-Exchange-Organization-SenderRep-Score: 3
X-MS-Exchange-Organization-SenderRep-Data:
 IpClassLargeGrayOther_GrayOther_unknown
X-MS-Exchange-Organization-VBR-Class: GrayOther
X-MS-Exchange-Organization-HMATPModel-Spf: 1
X-MS-Exchange-Organization-HMATPModel-Recipient:
 <PII:H101(yqtorCSoPDZ7HxoNinH3WMYg8E0ww9KuNPuN2UCOUoU=)>@chmsbc.org.br
X-MS-TrafficTypeDiagnostic:
    DM3NAM02FT021:EE_|CPWP152MB5144:EE_|CPWP152MB5144:EE_QuarantinedMessage
X-MS-Exchange-Organization-OrderedPrecisionLatencyInProgress:
    LSRV=CPWP152MB5144.LAMP152.PROD.OUTLOOK.COM:TOTAL-HUB=5.077|SMRE=1.453(RENV=0.149|REOH=0.150|REOD=1.029|CMSGC=0.123|R-HS=1.175(R-CMSG=1.175(R-HSXD=1.173
 )))|CAT=3.079(CATOS=1.460(CATSM=1.457(CATSM-Pre Index Routing
 Agent=0.513|CATSM-DC Pre Content Filter Agent=0.919
 ))|CATORES-INC=1.600(CATRS=1.600(CATRS-DC Pre Content Filter
 Agent=0.325|CATRS-DC Content Filter Agent=0.421 |CATRS-Spam Filter
 Agent=0.191|CATRS-Antispam Quarantine Agent=0.611)))|CAT=0.549
 (CATOS=0.312(CATSM=0.312(CATSM-Pre Index Routing
 Agent=0.299))|CATORES=0.218(CATRS=0.218 (CATRS-Index Routing
 Agent=0.198)));2023-07-14T13:15:58.260Z
X-MS-Exchange-Organization-MessageLatency:
 SRV=DM3NAM02FT021.eop-nam02.prod.protection.outlook.com:TOTAL-FE=1.129|SMR-PEN=0.844(RENV=0.294|REOH=0.548(SMREH=0.256(SMREH-Protocol
 Filter Agent=0.255 )))|SMS=0.286
X-MS-Exchange-Organization-MessageLatency:
    SRV=DM6PR06CA0005.namprd06.prod.outlook.com:TOTAL-FE=0.399|SMR-PEN=0.026(RENV=0.022)]SMS=0.373(SMSC=0.293)
X-MS-Exchange-Forest-ArrivalHubServer: CPWP152MB5144.LAMP152.PROD.OUTLOOK.COM
X-MS-Exchange-Organization-AuthSource:
    DM3NAM02FT021.eop-nam02.prod.protection.outlook.com
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-Exchange-Organization-FromEntityHeader: Internet
X-MS-Exchange-Organization-MessageScope: 7f8f1c1e-0d05-44c3-85bd-78eb09fce4db
X-MS-Exchange-Forest-MessageScope: 7f8f1c1e-0d05-44c3-85bd-78eb09fce4db
X-MS-Exchange-Organization-Antispam-ProtocolFilterHub-ScanContext:
    ProtocolFilterHub:SmtpOnEndOfData;
X-MS-Office365-Filtering-Correlation-Id: fa5ecd71-3443-4aee-354a-08db846c72ec
X-MS-Exchange-Organization-P2SenderPII:
    <PII:H101(OjjbWWinbPHc1DyyFntLJ4LzxRBHUJWWGBbC5f/Fqpk=)>@p7solucoes.net
X-MS-Exchange-Organization-Auth-DmarcStatus: Pass
X-MS-Exchange-Organization-Antispam-AuthResults:
    {"SpfDomain":"p7solucoes.net","SpfAuthStatus":"Pass","DkimAuthStatus":"None","DkimSubStatus":"None","DmarcAuthStatus":"BestGuessPass","DmarcAction":"None","A
X-MS-Exchange-Organization-PFAHub-Total-Message-Size: 3557763
X-MS-Exchange-Organization-OriginalSize: 3557763
X-MS-Exchange-Organization-Transport-Properties: DeliveryPriority=Low
X-MS-Exchange-Organization-IncludeInSla:
    False:FlexTransport:EnterpriseMsgsAboveSizeThreshold
X-MS-Exchange-Organization-Prioritization:
    2:FlexTransport:EnterpriseMsgsAboveSizeThreshold
X-MS-Exchange-Organization-HygienePolicy: Premium
X-MS-Exchange-Organization-ReplicationInfo:
    ReplicaId=183f333d-cf04-b256-670d-7b736c84db08;ReplicatingServerFqdn=CPUP152MB5148.LAMP152.PROD.OUTLOOK.COM
X-MS-Exchange-Organization-Antispam-PreContentFilter-PolicyLoadTime:
    PSOSUB:3;PSOSUBLOAD:2;PSOSUBRUN:0;PSOSUBCOUNT:0;SMORES:3;SMORESLOAD:2;SMORESRUN:0;SMORESCOUNT:0;SAORES:6;SAORESLOAD:1;SLORES:2;APORES:2;APORESLOAD:2;RSORES:1
X-MS-Exchange-Organization-MessageFingerprint:
    B589CAF8.1FA97788.78F12843.D89C00EA.200E6
X-MS-Exchange-Organization-FeatureTable:
    =?utf-8?B?ezM0MToxMTYsMzQyOjAsMzQzOjY2LDM0NDowLDM0NTo2NiwzNDY6MCwzNDc6?=
 =?utf-8?B?MTEyLDM0ODowLDM0OTo2MywzNTA6MCwzNTE6NjMsMzUyOjAsMzUzOjEzNywz?=
 =?utf-8?B?NTQ6ODAsMzU1OjE0OSwzNTY6OTAsMzY3OjM2LDM2ODo0LDM4NDoicDdzb2x1?=
 =?utf-8?B?Y29lcy5uZXQiLDM4NToicDdzb2x1Y29lcy5uZXQiLDM4NjoiVHJ1ZSIsMzg3?=
 =?utf-8?B?OiJUcnVlIiw0MjE6NDIsNDIyOjE4LDQyMzo0MiwwMjQ6MTgsNDI1OjQ2LDQy?=
 =?utf-8?B?NjoxMSw0Mjc6NDYsNDI4OjExLDQyOTozNyw0MzA6OCw0NTI6MSw0NTM6MSw0?=
 =?utf-8?B?NTQ6Ijc4RTVCRTkyQGNobXNiYy5vcmcuYnIiLDQ1NToiRkMiLDQ1NzoyODIs?=
 =?utf-8?B?NDU4OjcyNSw0NTk6OTUsNDYwOjEyMDQ2Nyw0NjE6MTE4LDQ2MjoSMjIxNSw0?=
 =?utf-8?B?NjM6MTE4LDQ2NDo5MjIxMSw1MDE6MSw1MDI6Nyw1MDM6Miw1MDQ6Nyw1MDY6?=
 =?utf-8?B?Miw1MDc6MSw1MDg6InSvbmUiLDUwOToicDdzb2x1Y29lcy5uZXQiLDUxMDoi?=
 =?utf-8?B?cDdzb2x1Y29lcy5uZXQiLDUxMToicGFzcyIsNTEyOjEwOSw2MDE6NjUsNjAy?=
 =?utf-8?B?OjgsNjAzOjYzLDYwNDowLDY1MToyLDY1MzoxLDY1NjoxLDY2NjoyNzEsNjY3?=
 =?utf-8?B?OjEwMTA2MTUwMzIsNjY4OjAsNjY5OjQ4LDcyMToiMi45NCIsNzIyOiIyLjU1?=
 =?utf-8?B?Iiw3MjM6MSw3MjU6Myw3MjY6Myw3Mjg6NTQsNzMwOjQyLDczNToiMi45MyIs?=
 =?utf-8?B?NzM4OjEsNzM5OjIsNzQwOjEsNzQyOjIsNzQzOjYsNzQ0OjEsNzQ5OiJMYXRu?=
 =?utf-8?B?Iiw3NTg6IkJEODlDQUY3LjFGQTU3Nzg4LjdCRjExQjgzLkQ4OUMyMEVBLjIw?=
 =?utf-8?B?MEREIiw3ODE6Miw3ODI6NDYsODM4OiJodG1sOjE7aGVhZDox0211dGE6MTti?=
 =?utf-8?B?b2R5OjE7cDoxMTticjo1IiwSNjQ6MTEsMTAxMDowLDEwMjg6MzY1LDEwMjk6?=
 =?utf-8?B?MzQ1LDEwMzA6MzI2LDEwMzE6MTksMTAzMjozNjUsMTAzMzozNDUsMTAzNDoz?=
 =?utf-8?B?MjYsMTAzNToxOSwxMTAxOiIwLjA3OSIsMTIyMzoiMiIsMTIyNDoiMSIsMTIy?=
 =?utf-8?B?NToiSSIsMTIyNjoiT2ZmaWNlIiwxNDAxOjAsMTQwMjowLDE0MDM6MCwxNDA0?=
 =?utf-8?B?OjAsMTQwNTowLDE0MDY6MCwxNDA3OjI2LDE0MDg6MjcsMTQwOTo0NiwxNDEw?=
 =?utf-8?B?OjQ4LDE0MTE6NDYsMTQxMjo0OCwxNDEzOjExLDE0MTQ6MjkSNTM3LDE0MTc6?=
 =?utf-8?Q?16,1418:45446478,1427:125,1428:43523432210}?=
X-MS-Exchange-Organization-Antispam-PreContentFilter-ScanContext:
    CategorizerOnSubmitted;CategorizerOnResolved;
X-MS-Exchange-Organization-AVScannedByV2: true
X-MS-Exchange-Organization-AVScanComplete: true
X-MS-Exchange-Organization-IsAnyAttachmentAtpSupported: true
X-MS-Exchange-Organization-ExternalRoutingTopologyAnalysis:
X-MS-Exchange-Organization-Recipient-Limit-Verified: True
X-MS-Exchange-Organization-TotalRecipientCount: 1
X-MS-Exchange-Organization-ASDirectionalityType: 1
X-MS-Exchange-Organization-HVERecipientsForked: 1.0
X-MS-Exchange-Organization-SafeAttachmentPolicy-Enable: 0
X-MS-Exchange-Organization-SafeLinksPolicy-EnableSafeLinksForEmail: 0
X-MS-Exchange-Organization-SafeLinksPolicy-EnableSafeLinksForInternalSenders:
    0
X-MS-Exchange-Organization-Boomerang-Verdict: None
X-MS-Exchange-Organization-MetadataFeatureTable:
    {756:0,757:0,1010:0,1036:"27715"}
X-MS-Exchange-Organization-HMATPModel-DkimAuthStatus: 7
X-MS-Exchange-Organization-HMATPModel-DmarcAuthStatus: 2
X-MS-Exchange-Organization-SenderIntelligence-P2Sender:
    {"stringProperties":{"Watermark":"2023/07/13","ListDisplayNames_30D":"","FirstSeen_30D":"2023-06-14","LastSeen_30D":"2023-07-
12","AvgInbound_1D":"1.03","AvgOutbound_1D":"0","VolumeBucket":"","_STATUS":"Success"},"numericProperties":
{"TotalEmailsSent_30D":31,"TotalDaysSent_30D":14,"SenderScore":698,"MoveToJunkCount":0,"P2SenderReputation":112,"TotalCountSum24h":4,"TotalCountSum1h":2,"EntityF
X-MS-Exchange-Organization-Rules-Execution-History:
    a4cec6b6-424b-4e20-b090-eff91e8921fb%%%eed77037-5967-4e4c-8630-26fd0feb054a
X-MS-Exchange-Forest-RulesExecuted: CPWP152MB5144
```

X-MS-Exchange-Organization-RulesExecuted: CPWP152MB5144
X-MS-Exchange-Organization-Antispam-AnalystFeatureFilter-ScanContext:
CategorizerOnResolved;
X-MS-Exchange-Organization-AttachmentDetailsInfo-ChunkCount: 1
X-MS-Exchange-Organization-AttachmentDetailsInfo-0:
=?utf-8?B?W3siSUQiOjAsIkZTIjo0NDkyNjgsIkhGSCI6IkdwHFdSeDl0bVpPOHd6ZEhF?=
=?utf-8?B?ZWh6WGxmNWJ5VFkxUG9TUC9HNEh5M0lEK2s9IiwiRkUiOiJwZGYiLCJBRlI6?=
=?utf-8?B?NTEyLCJBRlQiOiJ7NzgOOlwiYXRic3RhZG8gZGUgdmlzaXRhIGFzc2luYWRv?=
=?utf-8?B?XzAwMDEucGRmXCIsNzg5OlwicGRmXCJ9IiwiQUZUMiI6Ins3ODQ6XCJhdGVz?=
=?utf-8?B?dGFkbyBkZSB2aXNpdGEgYXNzaW5hZG9fMDAwMS5wZGZcIiw3ODk6XCJwZGZc?=
=?utf-8?B?In0ifSx7IklEIjoxLCJGUyI6MjE0Mjg0MSwiSEZIIjoibUtnOVhseE9MT0Jp?=
=?utf-8?B?Q2F1eWNMeWp2UHJ4b2xTSDJETWplSk1IQUZ4TlZaQT01LCJGRSI6InBkZiIs?=
=?utf-8?B?IkFGIjo1MTIsIkFGVCI6Ins3ODQ6XCJQcm9wb3N0YSBjb21lcmNpYWwgZSBw?=
=?utf-8?B?bGFuaWxoYSBvcsOnYW1lbnRhcmlhLnBkZlwiLDc4OTpcInBkZlwifSIsIkF6?=
=?utf-8?B?VDIiOiJ7NzgOOlwiUHJvcG9zdGEgY29tZXJjaWFsIGUgcGxhbmlsaGEgb3I=?=
=?utf-8?B?w6dhbWVudGFyaWEucGRmXCIsNzg5OlwicGRmXCJ9In1d?=
X-MS-Exchange-Organization-SenderRecipientCommunicationState: FC
X-MS-Exchange-Organization-Impersonation-FeatureData:
{1201:"DisplayNameManualList",1202:"multipass",1203:1,1204:0,1205:1,1206:2,1207:2,1208:2,1209:1,1210:"Include",1211:0,1212:"Office",1213:0,1214:0,1215:0,1216
X-MS-Exchange-Organization-MLModelHit: M3EPV
X-MS-Exchange-Organization-Antispam-ContentFilter-ScanContext:
CategorizerOnResolved;
X-MS-Exchange-Organization-CommunicationStateSummary: FC
X-MS-Exchange-Organization-FirstContactSummary:
ST=3;MRG=0;EXT=0;UN=1;DRCT=1;EV=1;FC=1;NESI=0;NES=0;ESTI=0;EST=0;INS=0;MP=0;UD=0;QE=0;ERR=0
X-MS-Exchange-Organization-CFA-UserOption: 0
X-MS-Exchange-Organization-CompAuth-Eop: compauth=pass reason=109
X-MS-Exchange-Organization-ContainsAttachments: true
X-MS-Exchange-Organization-Feature-Long: 0 201:862 202:353 203:1 205:3 206:3
208:54 210:42 215:848 235:2 236:7 238:2 239:1 240:2 241:1 243:2 244:6 245:1
246:1 247:1 248:1 252:1 255:1 256:2 257:46 1007:Latn 1014:none
1015:p7solucoes.net 1020:p7solucoes.net 1030:p7solucoes.net
1034:78E5BE92@chmsbc.org.br 1035:p7solucoes.net
X-MS-Exchange-Organization-ExtractionTagsSubject:
=?utf-8?B?RE9DVU1FTlRBw4fDg08gLSBSRUYuIFBST0NFU1NPIERFIENPTlRSQVRPUyBO?=
=?utf-8?B?wrowNTkvMjAyMy1DU1NCQw==?=
X-MS-Exchange-Organization-ExtractionTagsFrom: fabiofidelis@p7solucoes.net
X-MS-Exchange-Organization-ExtractionTagsSubjectNormalized: documentacao ref
proceso de contratos noos9 2o23 csbc
X-MS-Exchange-Organization-ExtractionTags: SUB64;
X-MS-Exchange-Organization-ATPDetonationContext: Email_Enterprise_Mailflow
X-MS-Exchange-Organization-AtpDetonationPriority: 1
X-MS-Exchange-Organization-Antispam-SpamFilter-ScanContext:
CategorizerOnResolved;
X-MS-Exchange-Organization-Antispam-AnalystRuleHits:
(13230028)(451199021)(1096003)(22186003)(6966003)(6916009)(28085005)(5660300002)(58800400005)(108616005)(33964004)(24736004)(356005)(86362001)(26005)
(9686003)(7636003)(224303003)(6266002)(21480400003)(336012)(36756003)(7596003)(2616005)(7126003)(43356004)
X-MS-Exchange-Organization-Antispam-ScanContext: DIR:Incoming;SFV:NSPM;SKIP:0;
X-MS-Exchange-Organization-FeatureTableV2:
=?utf-8?B?ezM0MToxMTYsMzQyOjAsMzQzOjY2LDM0NDowLDM0NTozNiwzNDY6MCwzNDc6?=
=?utf-8?B?MTEyLDM0ODowLDM0OTo2MywzNTA6MCwzNTE6NjMsMzUyOjAsMzUzOjEzNywz?=
=?utf-8?B?NTQ6ODAsMzU1OjE0OSwzNTY6OTAsMzY3OjM2LDM2ODo0LDM4NDoicDdzb2x1?=
=?utf-8?B?Y29lcy5uZXQiLDM4NToicDdzb2x1Y29lcy5uZXQiLDM4NjoiVHJ1ZSIsMzg3?=
=?utf-8?B?OiJUcnVlIiw0MjE6NDIsNDIyOjE4LDQyMzo0Miw0MjQ6MTgsNDI1OjQ2LDQy?=
=?utf-8?B?NjoxMSw0Mjc6NDYsNDI4OjExLDQyOTozNyw0MzA6OCw0NTI6MSw0NTM6MSw0?=
=?utf-8?B?NTQ6Ijc4RTVCRTkyQGNobXNiYy5vcmcuYnIiLDQ1NTo1RkM1LDQ1NzoyODIs?=
=?utf-8?B?NDU4OjcyNSw0NTk6OTUsNDYwOjEyMDQ2NywwNjE6MTE4LDQ2Mjo5MjIxNSw0?=
=?utf-8?B?NjM6MTE4LDQ2NDo5MjIxNSw1MDE6MSw1MDI6NywwMDM6MiwwMDQ6NywwMDY6?=
=?utf-8?B?MiwiMDc6MSw1MDg6ImSvbmU1LDUwOTo1cDdzb2x1Y29lcy5uZXQiLDUxMDo1?=
=?utf-8?B?cDdzb2x1Y29lcy5uZXQiLDUxMToicGFzcyIsNTEyOjEwOSw2MDE6NjUsNjAy?=
=?utf-8?B?OjgsNjAzOjYzLDYwNDowLDY1MToyLDY1MzoxLDY1NjoxLDY2NjoyNzEsNjY3?=
=?utf-8?B?OjEwMTA2MTUwMzIsNjY4OjAsNjY5OjQ4LDcyMToiM145NCIsNzIzOjEsNzI1?=
=?utf-8?B?OjMsNzI2OjMsNzI4OjU0LDczMDo0Miw3MzU6IjIuOTMiLDczODoxLDczOToy?=
=?utf-8?B?LDc0MDoxLDc0MjoyLDc0MzoZLDc0NDoxLDc1NjowLDc1NzowLDc1ODoiQkQ4?=
=?utf-8?B?DUNBRjcuMUZBNTc3ODguN0JGMTFCODMuRDg5QzIwRUEuMjAwREQ1LDc4MToy?=
=?utf-8?B?LDc4MjowNiw4Mzg6ImhbbWw6MTtoZWFkOjE7bWV0YToxO2JvZHk6MTtwOjEx?=
=?utf-8?B?O2JyOjUiLDEwMTA6MCwxMDI4OjM2NSwxMDI5OjM0NSwxMDMwOjMyNiwxMDMx?=
=?utf-8?B?OjE5LDEwMzI6MzY1LDEwMzM6MzQ1LDEwMzQ6MzI2LDEwMzU6MTksNTAzNjoi?=
=?utf-8?B?Mjc3MTU1LDExMDE6IjAuMDc5IiwxMjIzOiIyIiwxMjI0OiIxIiwxMjI1OiJJ?=
=?utf-8?B?IiwxMjI2OiJPZmZpY2UiLDE0MDE6MCwxNDAyOjAsMTQwMzowLDE0MDQ6MCwx?=
=?utf-8?B?NDA1OjAsMTQwNjowLDE0MDc6MjYsMTQwODoyNywxNDA5OjQ2LDE0MTA6NDgs?=
=?utf-8?B?MTQxMTo0NiwxNDEyOjQ4LDE0MTM6MTEsMTQxNDoyOTk1MzcsMTQxNzoxNiwx?=
=?utf-8?B?NDE4OjQ1NDQ2NDc4LDE0Mjc6MTI1LDE0Mjg6NDM1MjM0MzIyMTAsMjUwMTow?=
=?utf-8?B?LDI1MDI6MCwyNTAzOjAsMjUwNDowLDI1MDU6MCwyNTA2OjAsMjUwNzowLDI1?=
=?utf-8?B?MDg6MCwyNTA5OjAsMjUxMDowLDI1MTE6MCwyNTEyOjAsMjUxMzowLDI1MTQ6?=
=?utf-8?B?MCwyNTE1OjAsMjUxNjowLDI1MTc6MCwyNTE4OjAsMjUxOTowLDI1MjA6MCwy?=
=?utf-8?B?NTIxOjAsMjUyMjowLDI1MjM6MCwyNTI0OjAsMjUyNTowLDI1MjY6MCwyNTI3?=
=?utf-8?B?OjAsMjUyODowLDI1Mjk6MCwyNTMwOjAsMjUzMTowLDI1MzI6MCwyNTMzOjAs?=
=?utf-8?Q?2534:0,2535:0,2536:0,2537:0,2538:0,2539:0}?=
X-MS-Exchange-Organization-Antispam-PostContentFilter-ScanContext:
CategorizerOnResolved;
X-Forefront-Antispam-Report:
CIP:201.76.49.53;CTRY:BR;LANG:pt;SCL:8;SRV:;IPV:NLI;SFV:SPM;H:mail4953.hm1315.locaweb.com.br;PTR:mail4953.hm1315.locaweb.com.br;CAT:HPHISH;SFS:(13230028)
(451199021)(1096003)(22186003)(6966003)(6916009)(28085005)(5660300002)(58800400005)(108616005)(33964004)(24736004)(356005)(86362001)(26005)(9686003)(7636003)
(224303003)(6266002)(21480400003)(336012)(36756003)(7596003)(2616005)(7126003)(43356004);DIR:INB;
X-MS-Exchange-Organization-Cross-Session-Cache:
=?utf-8?B?MDB0SVA9MjAxLjc2LjQ5LjUzOBVJUEMwPTIwMDQsMjA1NSw5NTAsOTUxLDIw?=
=?utf-8?B?MDUsMjAwNiwyMDA3LDIwMDgsMjAwOSwyMDEwLDIwMTEsMjAxMiwyMDEzLDIw?=
=?utf-8?B?MTQsMjAwMCwyMDUwLDIwNTEsMjA1Miw5NTIsOTAyLDIwNTQsMjAxNiw5MDMs?=
=?utf-8?B?OTA1LDE3NzYsOTAxLDkwNCwyMDAzLDIwMDEsMzAwMCwxNzczLDIwMDIsOTY3?=
=?utf-8?B?LDIwNTgsMjA1OSwyMDYwLDUzMSwyMDE3LDUwODAsNTAwMSw5MDYsNTAxMCw1?=
=?utf-8?B?MDExLDUwMDIsNTAwMyw1MDA1LDUwNzA7TUlQQzA9OTUwLDk1Miw5NTE7UkVQ?=
=?utf-8?B?PTtTTD0xO0VNU0w9MTtTQ0w9ODtCTD0wO1JMPTE7UEIEPTA7RVhQSUQ9O0lZ?=
=?utf-8?B?SW5jb21pbmdNYWlsPXRydWU7VElQPU5vdExpc3RlZDtDSVBDUlk9QlI7U0FV?=
=?utf-8?B?VEhPUD0xO1JNWD1PZmZpY2UzNjU7UkVDSVB3RUSURE9NQUlDX095SUc9Y2ht?=
=?utf-8?B?c2JjLm9yZy5icjtFSVBOMT0yMDA0LDIwNTUsOTUwLDk1MSwyMDA1LDIwMDYs?=
=?utf-8?B?MjAwNywyMDA4LDIwMDksMjAxMCwyMDExLDIwMTIsMjAxMywyMDE0LDIwMDAs?=
=?utf-8?B?MjA1MCwyMDUxLDIwNTIsOTUyLDkwMiwyMDU0LDIwMTYsOTAzLDkwNSwxNzc2?=
=?utf-8?B?LDkwMSw5MDQsMjAwMywyMDAxLDMwMDAsMTc3MywyMDAyLDk2NywyMDU4LDIw?=
=?utf-8?B?NTksMjA2MCw1MzEsMjAxNyw1MDgwLDUwMDEsOTA2LDUwMTAsNTAxMSw1MDAy?=
=?utf-8?B?LDUwMDMsNTAwNSw1MDcwO01JUEMxPTk1MCw5NTIsOTUxLDkwMiwyMDE0LDUw?=
=?utf-8?B?ODA7QT0wMTtNWD0wMDtQVFI9MDBtYWlsNDk1MySobTEzMTUubG9jYXdlYi5j?=
=?utf-8?B?b20uYnI7U1BGPWIwMTExWm1GaWFKOW1hV1JsYkdselFIQTNjMjlzZFd0dlpY?=
=?utf-8?B?TXVibVYwO0RLSU09O0RNQVJDPTAyY0RkamIyeDFZMjlsY3k1dVpYUT1cOztB?=
=?utf-8?B?VVRIUkVTPVttteC5taWNyb3NvZnQuY29tLDFdezUsMSxVQUJoQUhNQWN3QT0s?=
=?utf-8?B?Y3dCbEFHNEFaQUJsQUhJQUl0QkpBRkFBSUFCcEFIYUFJQUFSQUR0QU1RQXVB?=
=?utf-8?B?RGNBTmdBdUFEUUFPUUF1QURVQU13QT0sY3dCdEFIUUFjQUF1QUhJQV13QndB?=
=?utf-8?B?SFFBVkFCdkFFUUF1d0J0QUdFQWFRQnVBQT09FF13Qm9BRzBBY3dCaUFHTUFM?=
=?utf-8?B?Z0J2QUhJQVp3QXVBR01BY2d0PSxjd0J0QUhRQWNBQXVBRTBBWVFCcEFHd0F5?=
=?utf-8?B?Z0J5QUc4QWJRQT18Y0FBM0FITUF1d0JzQUhVQVl3QnZBR1VBY3d0dUFHNEFa?=
=?utf-8?B?UUIwQUE9PX17OSwxNyxRZ0JsQUhNQWRBQkhBSFVBWlFCekFITUFVQUJoQUhN?=
=?utf-8?B?QWN3QT0sLF1RQmpBSFFBYVFCdkFHNEF0VGdCdkFHNEFaUUE9LGF0QmxBR0VB?=

=?utf-8?B?WkFCbEFISUFMZ0JtQUhJQWJ3QnRBQT09fGNBQTNBSE1BYndCc0FIVUFZd0J2?=
=?utf-8?B?QUdVQWN3QXVBRzRBWlFCMEFBPT19ezIsNyxUZ0J2QUc0QVpRQT0sYlFCbEFI?=
=?utf-8?B?TUFjd0JoQUdjQVpRQWdBRzRBYndCMEFDQUFjd0JwQUdjQWJnQmxBR1FBfXsx?=
=?utf-8?B?Miw3LFRnQnZBRzRBWlFBPSxNQUE9fTtQMkJ0TFByZWZlcnJlZEhNQUNDZXJ0?=
=?utf-8?B?SWQ9MTA4O1NwZlJlc3VsdD0xO0RraW1TdGF0dXM9NztEa2ltU1M9MDtEbWFy?=
=?utf-8?B?Y1N0YXR1cz0yO0RtYXJjQWN0aW9uPTA7QVJDUkVTPXYxMDAwMDAwMDAwMDAw?=
=?utf-8?B?MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA7QXJjT3ZlcnJpZGVEbWFy?=
=?utf-8?B?Y0ZhaWx1cmU9MDtDQXVBaEV4cD10cnV1O18SZV30PTE7QVRDSEM9MjtJc0Fu?=
=?utf-8?B?eUF0dGFjaG1lbnR0dHBTdX0wb3J0ZWQ9dHJ1ZTtVUkxDX0JFPTA7VVJMQ19C?=
=?utf-8?B?RUM9MDtVUkxDX0FFPTA7R1B5PUI1OD1DQUZCLjFGQTk3Nzg4LjdCRjEyQjQz?=
=?utf-8?B?LkQ4OUMwMEVBLjIwMEU2DIRETkE9QkQ4OUNBRjcuMUZBNTc3ODguN0JGMTFC?=
=?utf-8?B?ODMuRDg5QzIwRUEuMjAwREQ7Tm9ETHg9MTtDR0RRMeFN1cHBvcnRlZD0xO1RN?=
=?utf-8?B?RF9TUz0xO1RNRF9BT1Q9MjEyNjtUTURFQ1NVTT0zMDg5O1RNRF9EVEFFVD0x?=
=?utf-8?B?O1RNRF9FUz0wO1RNRF9UVD0wO1RNRF9ETUSTUE09MTI1OTY7VE1EX0RNUl8N?=
=?utf-8?B?PTEyMDtUTURFUFNBVFA9MDtUTURFUFM9OTYwO1RNRF9TQ05UPTM7VE1EX1RT?=
=?utf-8?B?QVRQPTA7VE1EX1RTPTA7VE1EX0FUUFAyPUZhbHN1O1RNRF9DST1lb11CUjtU?=
=?utf-8?B?TURFQ0Q9MjAxNy0wOS0xNSAxOTo1NjoyOC4wMDA7VE1EX05FV1Q9MDtUTURF?=
=?utf-8?B?TkVXVFQ9MDtUTURFUVM9MTtUU19TUz0xO1RSX1NNQVM9MDtUU19UTUFTPTA7?=
=?utf-8?B?VFJfVU1BUz0wO1RSX1RUVTI0SD0wO1RSX1RUMjRIPTA7VFJfQUZXUjI0SD0w?=
=?utf-8?B?O1RSX0SEU1NQTVIyNEg9MDtUU19SMUg=?=
X-MS-Exchange-Organization-Cross-Session-Cache:
=?utf-8?B?MDE9MTAxO1RSX1IyNEg9MjM3O1RSX1NQTVIxSD0wO1RSX1NQTVIyNEg9MDtU?=
=?utf-8?B?U19VUDFSMUg9MDtUU19VUDFSMjRIPTA7VFJfVVAxU1BNUjI0SD0wO1RSX0JD?=
=?utf-8?B?VFI9RmFsc2U7VFJfUVM9MTtCU19WPU5vbmU7RE1SPTE7UFRSTz1sb2Nhd2Vi?=
=?utf-8?B?LmNvbS51cjtQMk89cDdzb2x1Y29lcy5uZXQ7UF9DQVVUSD1wYXNzO1BfQ0FV?=
=?utf-8?B?VEhSPTEwOTtTSVAyQkNMQVA9LTE7U01QMkJOTEFGPS0xO0JVTEtGX0RCRz1Q?=
=?utf-8?B?M1NOQXxUUF9CVDo3O0NGUD1jOTE5N2YxZS1jNDk5LTQzZmMtYmU2Ni0zMjZ1?=
=?utf-8?B?NDg0Mjg3ZDc7SENGUD0yZDMyMDUzYy01Yzk0LTQ4ZDMtYWQ1YS1mYzk0MDYz?=
=?utf-8?B?NjIkMjk7SENGUEM9MCw3O01GUD00ZGJhZjNjZC1mYTk2LTQ5NzgtYmNhNC0x?=
=?utf-8?B?ZmJkYTNkZGQxYTg7QVBQPTE4MmQwMmRhLTJiMjMtNGNiMy1iYTZkLWM1MGRh?=
=?utf-8?B?ZmQ5NjdmNTtBUFBDPTExMDA7R1dTX1JlYWQ9VjI7U1JDUz1GQztSZXBEYXRh?=
=?utf-8?B?VmVyPUVPUDtDQVVUSD1wYXNzO0NBVVRIUj0xMDk7Q0FVVEhfQ0FUPUFEO1RE?=
=?utf-8?B?SU1QX01NUERfREJHPVNLUC5ESVM7T0RJTVBfSU1QRF9EQkc9U0tQLkRJUztJ?=
=?utf-8?B?TVBVX0RCRz1TS1AuRE1TO01NUERfREJHPVRESU1QKFNLUC5ESVMpLE9ESU1Q?=
=?utf-8?B?KFNLUC5ESVMpO01WQ19EQkc9RE05fDI8MXx3fE9mZmljZXxMO1MxO0JNRVNW?=
=?utf-8?B?PTc5NztCTUVTV19GUD03OTc7Qk1FU1ZfVkVSPTE7TUxGX0RCRz1CTUVTV1M3?=
=?utf-8?B?OTcjMXxCTUVQV1MzMzUjMXxNM0hQV1MxIzF8TTNFUFYjMTIjMSMzMHxNMBVT?=
=?utf-8?B?V1MwMzEjMTtCTUVQVj0zMzU7Qk1FUFZfR1A9MzM1O0JNRVBWX1ZFUj0xO0NN?=
=?utf-8?B?SFBWPTQ2NDU7TTNIUFY9MTtNMBhQV19GUD0xO00zSFBWX1ZFUj0xO00zRVBW?=
=?utf-8?B?PTEyO00zRVBWX0ZQPTEyO00zRV9WX1ZFUj0xO00zRVNWPTEzMTtNM0VTV19G?=
=?utf-8?B?UD0xMzE7TTNFU1ZfVkVSPTE7Q0xFUFY9MTE7VVJMR19EQkc9U0tQRDoxO0ZT?=
=?utf-8?B?Qz0zMTtGU0NJRD05MzAxMDkwMTYxfDIwMjIwMjI4MDAwOTY7UFZFQ090Rj1I?=
=?utf-8?B?SUdIO1BWX00zPVBIUztBU0M9MTtBU0NJRD00MzM1NjAwNDtQV19NTEY9UEhT?=
=?utf-8?B?O1BWX01MR19DTD04O1BWX01MR19GQz1NMzYwO1BWX0ZNPVBIUztQV19GQz1N?=
=?utf-8?B?TE1vZGVsO1BWX0NMPTg7UFZfUEFDVD1IUEhJU0g7RkZNPVBIUztGR1ZFQ0w9?=
=?utf-8?B?ODtGVl9QQUNUPUhQSElTSDtGVj1QSFM7RlZTPUZpbHRlcnM7RlNDTD04O1RB?=
=?utf-8?B?UF9FUD1IUEhJU0g7VEFDVENBVD0xNTtUQUNUPTU7VEFDVF9JRD0yZDMyMDUz?=
=?utf-8?Q?c-5c94-48d3-ad5a-fc9406369d29?=
X-Microsoft-Antispam: BCL:0;
X-Microsoft-Antispam-Message-Info:
=?utf-8?B?Q31FYzMxST1RTDVsZzh2UGIzcUhroEVRVDYyWEZ0TEhuU1hqbVZyeERGTC9G?=
=?utf-8?B?SzRLQmZTYUROWnEyMnhQZWRPYTMxd2lDbVBPTm02Vmlnc1NSamh1cDFLWndL?=
=?utf-8?B?R042YjdxcOFIMk9DRGpTWVA0MmVNN10GdW9ZYUFSb3RLYmswUnUrS1EzekRx?=
=?utf-8?B?b0ZLRDR1YkI1YmVvWXNicjdwZ3h1M3dXSTI0M2hJcEY0NEJDS1RqV1JsTU9N?=
=?utf-8?B?L05DK3JwM3F6cmZ2SVNZaGU0MVJXSkU1d1poQntFNzI0ZU91T0c3V05ZWE1m?=
=?utf-8?B?ZzdSaU1kTVUwTm1YamQ4K3I0d09OR2dRV2c1eS9JZXJYS05GUmdqMU1ucHBZ?=
=?utf-8?B?SGxrVmFnMmRycWpFd1E0M2lrNahjM1dwdVkvcmlMSzhBZzFGYjllamZuS2Zh?=
=?utf-8?B?RHFlSk5STEJxNjlKelhLWmZtamhISUhvS2V3TzFQYmIxQUNKSG1oc0E1M05x?=
=?utf-8?B?eWg3L1d2R2SJdHJSUCtXUmhMN2ZBekVBTU9SK0hkck5OeOd0N10OZGUwSHds?=
=?utf-8?B?TTV1UENzUzFVeXRtaTQwYUFzNEdBdWxoZHVJTzZhS3RsMkFCZnVKSU1LS3JU?=
=?utf-8?B?SzVHT1BjZVpINHN0d1ZvT2hjR2VBUzNwYjd4L0VPN301dGVTYjcvU1NxS1Zo?=
=?utf-8?B?RjArbTVEL3hSQXUrOHg3SjhDZUxyZyt6RTVUSnlrbGRtVEsya6lPcEt0L004?=
=?utf-8?B?Z0Zn505FVjRHSGh4cW5UK2RXOUJJSDFHb0dvaUhZUDVZS2RJcWpOVnFCYzZM?=
=?utf-8?B?NkwrdjRXMjc1aklpQk1uZzNsVTdUcWd4SVVIanVSd1kveEdsZ1NPWFE3Z01z?=
=?utf-8?B?ZzM5ZH1FY1VkbmtJOHh6cWJPMForYzZQcFpQd3E3SWk1WENkQkVSMFowYVpJ?=
=?utf-8?B?WWRzYjROTGlYUXBVRFZTNDhKalVUYUFsQTM2T3JaMCtFUk41WWxsNEg1TENR?=
=?utf-8?B?c11SRDZvRzM1Z2MxaEtWVkMyZC9mRktOT21YZStmaE1hcHJzcnBsUTJPSV15?=
=?utf-8?B?MWcxSWdWeDVoMVZoV1ZLMD1PZFJhNG9OL1JvdHVNcHZPYXdENESMWG5lam1a?=
=?utf-8?B?a0ZHdWp3MFBZY1NUM1hjeSs2WGt1NVRnNjMwRHhtQU16Wlp5YWl6MG5nV0Ja?=
=?utf-8?B?ZUJJM1RlaDF4SjFjb2pBV0E5cES4eVhERnNnQmVBMzdNV0SkbzJPTXNHOFpW?=
=?utf-8?B?bGV2blNMMDU0aG16aitsNCtwZjNFOUxpSHRRdVdaL21nWjlRVXR0ZDRDTVZk?=
=?utf-8?B?eEdXZVFMSnJteE9KN1V2NTJabU9qK0tIc3pDVzdNcEczRWdZcHVpZ1dtcnFF?=
=?utf-8?B?dHk3dHVGMUhmaEQrbBg4aXVZZnh0aUpPRjJXd1RsR1NEckxUTE1EbENRTkd3?=
=?utf-8?B?V2dLTnYrTytBekZTYjBEQmNCSU9JVWVkM1lSQjBUQmVDU01rRkZOWTNEQzJ0?=
=?utf-8?B?VEdLK3NMT21aN3BMbFcyMmZaT3RKd1RWZVduT0N0cWtVQ0xubi10blpDbTNq?=
=?utf-8?B?YUtxL2x6V2IreWFLSGw2VnhEdXRaTnN1NDZzN21jRDVVWXI5eFE5NVFub2c4?=
=?utf-8?B?SmJZSEpIRHhpUVdSQ2xuSmRVTzBwUTVvWm1KZU9pNX0zWGJWN1c4R25mMzRH?=
=?utf-8?B?WmRyN1hYT2BzRU5sc2BwZnQzWXVHYjUvRXNHNBI35HJmV1ZoZ2dqTjJGc1FG?=
=?utf-8?B?M1ZJK2RRYm9EcUhkZHNNL0M5RUhPejFBU013bXZ1d2hRV2oxdVVoQWNUaGVL?=
=?utf-8?B?NVVTOWVaWXJveG1kcDJVNzRtanVNSUUrMn1EM1JjdTU1dFgvWHFMbX1SUkY0?=
=?utf-8?B?dnIwa2xVN2RYMnNEWG4vRzBhMDBkVHJPRXJuTGlmbnZJU1dsVnRVWGtGZFpI?=
=?utf-8?B?clAyaG5vRm5oYnJvNXk0YkSLOFg4dUNVUXRzV25URVZWbTISQUFhQ2pFckpL?=
=?utf-8?B?R1ZpVEVKa3Z4Zytuaj15WFNwR3E0RFBFZmVWYWpEY31QMUxGTVY0V0VoWmdh?=
=?utf-8?B?N1k1djFGVXY2SVJYblUzNUdXcDF5KzdCRHVCUG9FcVZoRTNqS0RPVWx1MUpk?=
=?utf-8?B?cGR1YzUxRGdFZms2bnVIWVRvckRtY0xIMVZzT1Z0bEtKb0hUS59mTnpjTU1y?=
=?utf-8?B?em5qdGZWOTFpaCBxVkRraG02Y212YXpjc3VJUjNtRWVxaTdZRHphOFRXWUNu?=
=?utf-8?B?NUtCb0RObDlLQ1djc1ZVTEtLMTV6QUtSaVF3TzkwRWtodnZkblV4Q3FpQWx4?=
=?utf-8?B?a1c2RWFFN0kvck1SZF1pYXA2SXdZb3phZjk5ODhsaEd1QUdTdVU2UGN1S3VS?=
=?utf-8?B?UWh0SVJXVzF3WjNmcmE4RWxhT1R2UWZjSGpBZmxhQ3UxUG3MWFkwSFEzT11w?=
=?utf-8?B?ejNUdnJWMUxUYjU5RE1iTVg1Qk8zN0dNYWZZQ1hrdU4zZ1BIcXNtNZ12QjYz?=
=?utf-8?B?N1NnNVVXUmhEWERrUDRZK2d1Nys2ZmMzemYwU3padjBVTGZqVk05aWFHRVAy?=
=?utf-8?B?cWFhNExQd1ZxU1hWYTFQRS94QWJHcGc5T0ZQdUc1Njd4emFOMjRIbytOdklT?=
=?utf-8?B?WFBqU1pTdmlhNVEzQT3xZ01JS2ZvcnJUZzFwZ1Naa21wTS9FUnZiV2I4OWt0?=
=?utf-8?B?VnM0aVdmbEJDVDRFRit4ZkVxQj1NdWQzU01VTE9oczhKck1KWDNnTUdPQ0da?=
=?utf-8?B?dVBjRUF5RkdCZ2R0R2tqeW5DdExCQ1hmV1BSaGVoMksxNUZVZUt8OU1sd1RU?=
=?utf-8?B?OXBsolNNQzJvMjJHSjlGQ2toaUdxR0V1c29qV2hGT1ORV211U2hSN3F0UWhq?=
=?utf-8?B?TzVMV241TW5kZEIzSWgrYjY0QUR2eFhROVRTVlpsbzRxZWF5ZDFLWEV2d0pO?=
=?utf-8?B?NkphUlRPWkEwOHVML1hTQz02UkFES3o1MGJuY1I3WnhXVVJKa1V5eU1hWWNN?=
=?utf-8?B?VUpYeTA1TTBZZGdtWHdCMXRBK2thQk9NZU1pS1dhdmREVEJZM0E9PQ==?=
X-MS-Exchange-Organization-Hygiene-SendToQuarantineStore:
v:2;f:HighConfPhish;r:15;e:False;n:Default;q:0;i:2d32053c-5c94-48d3-ad5a-fc9406369d29;t:HostedContentFilterPolicy;g:AdminOnlyAccessPolicy
X-MS-Exchange-Organization-TransportTrafficType: Email
X-MS-Exchange-Organization-TransportTrafficSubType: QuarantinedMessage
X-MS-PublicTrafficType: Email
X-MS-Exchange-Organization-GroupForkPerf: WCL=0;VL=0
X-MS-Exchange-Organization-Hygiene-QuarantineForkId:
9f934390-826f-47e3-64cc-08db846c7660
X-MS-Exchange-Organization-Hygiene-QuarantineMailMetadataInfo:
SQA=SUM|T=HighConfPhish|RD=15|EF=0|PID=2d32053c-5c94-48d3-ad5a-
fc9406369d29|PT=HostedContentFilterPolicy|ERN=RGVmYXVsdA==|EQT=QWRtaW5Pbmx5QWNjZXNzUG9saWN5|FID=9f934390-826f-47e3-64cc-08db846c7660|SM=|IR=|QS=1
X-MS-Exchange-Forest-Language: pt
X-MS-Exchange-Forest-IndexAgent-0:

AQ0CcHQBH+YEW3sNCiAgImluZGV4IjogMiwNCiAgIkF0dGFjaG1lbn
RQcm9wZXJ0aWVzIjogew0KICAgICJleHRlbnNpb24iOiAiVW5rbm93
biIsDQogICAgInVybHMiOiBbXSwNCiAgICAiaW5uZXJGaWxlcyI6IF
sNCiAgICAgIHsNCiAgICAgICAgIkZpbGVOYW1lIjogIiIsDQogICAg
ICAgICJGaWxlRm9ybWF0IjogImVtbCIsDQogICAgICAgICJGaWxlRX
h0ZW5zaW9uIjogIiINCiAgICAgIH0sDQogICAgICB7DQogICAgICAg
ICJGaWxlTmFtZSI6ICJhdGVzdGFkbyBkZSB2aXNpdGEgYXNzaW5hZG
9fMDAwMS5wZGYiLA0KICAgICAgICAiRmlsZUZvcm1hdCI6ICJwZGYi
LA0KICAgICAgICAiRmlsZUV4dGVuc2lvbiI6ICJwZGYiDQogICAgIC
B9LA0KICAgICAgew0KICAgICAgICAiRmlsZU5hbWU1OiAiUHJvcG9z
dGEgY29tZXJjaWFsIGUgcGxhbmlsaGEgb3LDp2FtZW50YXJpYS5wZG
YiLA0KICAgICAgICAiRmlsZUZvcm1hdCI6ICJwZGYiLA0KICAgICAg
ICAiRmlsZUV4dGVuc2lvbiI6ICJwZGYiDQogICAgICB9DQogICAgXS
wNCiAgICA1ZGV0ZWN0ZWRGb3JtYXQiOiA1Z3ppcCIsDQogICAgImSh
bWUiOiA1VW5rbm93biIsDQogICAgInR5cGUiOiAiU3RyZWFtQXR0YW
NobWVudCINCiAgfQ0KfV0AAYQUAAAPAAADH4sIAAAAAAAEAJ1YS3Pb
VpYG+BYk2E717GZzzUoNJQ0Ak3oL71GGougUibKokJInSftRCAkqSE
GAG1TV1tWqykwWqXSVd5PN1Cz18cLVXeVVkK06K+OHzXznXICinEy3
Z2wKwn2de8S3vvOg/ntV17bDE9H3MGEIoWu61nWPx65wT4QTuOehEP
2wNz5xg5ETv4xfhCJyB26EoSucUJxGYe8dDkMRvP6xurpSZ6m6tCwa
3eS2QSi61giDUe5kB/sk9DAyh45wh6duz3N876nTdwTdFX4SOUPR88
48PKHPIIwCbKF76aSunTij+E+Rh02uOIE4E7MmHxOnDh7uudsby4vo
Jsg95Yt/cIciwKn4eeTilwFFoBDRNShzzq/Y7oij7a544PnO6JKAA7
cFhYDj1PXJROcpK1+rEkpOYTFKpjlIwtNwOHJEIzxxIz1nXfCdwPM/
dUQ7ilB6D80UF8lqfeTiU39FwloPAuT5+4AKt9LrkCOvv6Xhmz55/e
3/2yni7XyCG/62U8Tb+4Q8/ptOEROf0Pb/o1MkTr/klb/mFInvLznl
9bcp9tc8s/tQ12qRrtX3mx+GD3wf0uuHze5hfacNJ+408XjQ6h62O6
26rk0coWuBX8LVY3aF2egO2RVvBghIe50UMD7BA3160l7QtTF9wNHh
whzsIGaTL3QNviBXkCeuHNF3p50AH0gXJ05wE/z7ztH2kKAn58l4Yx
x4fafv/m7sxq+w+ThCDIWkz61PWYKuE0Mn/pHVGZI52yQp6vMadjon
p6G8914YQP8Td2LuwOulnNA1EKoXYIINOfeOcSa9BuRyd0gM1zUvGI
6isbSab3PNQxkYQ7pAEsSN4ldhP+WIrs0TTRagc8R5/X8YgbPcnu9E
pN7pMsg6gFiDIOdwgG/2D3bZcbCzvFgOy5WTs8wE8TdL/gd7l+HIfP
wBkIOrwnHNGn9WqRjIR8aiYVu1R42t12w8bF17uEgqmaYwTflb16wK
hztw+PTKiaSGH/aQQ9jngFkMXSgPk89C/wzWMEHCIaajMy9+KW2FJc
JhjskhhWsY9LEef8949nwP3Aj9+LvjBNXTKP7ulIKWtiNxHHsk2pUe
HIUkYkqK9AoC8wx6j1XB+uSysU90YIEU6tcSsMAro1hz+DM3NbMnSR
/CBY32/YD91oftJNK69aOdQ3DAD8+jkygAh9vt+JkXDQbxC+x5/TL+
t3C7iTCOvwh2MLHfvt8UO/X0h5KwBzzoNLvN/cP6/iGJ3KmL5n2aqs
MZ9W63tV8/POrUaaUtfmGzrvH2t9rbaO8fduoBY5e2ND9s18SU+D/W
gk+33hbbzc5+vSNTRFs06vcPoH38dTn+Kf62LADZSLjRuIwMfuywI2
vWavyKCIOfbceLmKb14XAcpAjTSvfnYdagMBN3RPcAGjUP7OrmxmrV
XF2tcmz92bcpFGq1BfxaWVSdNmur1WoSr7gpFXUVr75vmqH179qhux
QuL5PNHsTPjz0k6+UV1q3lFRAgjIZhHI6/CpsgVT2kvJakSezoyqTQ
jZ9joYnlpdRG/Kj7Z05i8dTVU1ZAU65aC4xH7TocvwOG8yKwpoIcoU
XAca+109xrdUW3tfegzp5pH30M8lxAPmH+28HAK1fwMD3f8/mCcrmH
yfjF+ijcA7FhHLGj1Tn5TNeMVqz1zXVjbXOzUoVqlSWAWD+zxN7Ye4
qLo0+HOGfg0R6JDiq19ZWNbw1KKLX1WhUGt/BaMbkXHIVBr+0OTfbX
yup6jWSKUbJnCMLj90Fn7IeV4QFZu4sfn6bajWa3y4xLuNjuin2rLN
Kqr2t7nFP618LzWnDav1hmURFhzaEHZ1HOB5dr5sbKqiF+Tji40wGa
Kxq2M1nbfvzq5NTrVf3gjf5MpgduWbxEl7FMFCGmRs4JvXGmcjErjv
3wE+6twKLOu6JW27CWllaNzXUmCKdPylB992no4f3EQw4V/fFTWkFn
omtnVN0w1/OCHrVKlMVcEYSU8qjpGLpY7tHgLBwuGGhgRtCLGg1HDM
MTR680iCgY+yPvIJfFKkFRajgUKI4jFFKPc58TDimBO8EIbcTIg0wp
xL+1REiVEz1KUjWne9u0elPgUPE2oKY4c/wwEon11Zq1Vls3NuALV2
zvtN7cAYLVhLVW3TBqSwY3XSh5fa7UglqK07QPQlKe7oQostOmqsm+
+iq1smvFFVlKd9ynXAaooNL3lVbVa5HQiTsGwZ3MadKWUf5ZYyFdVC
12QCIJASSCCPUnPUbIHIM6wNGRSE1xKCk1YxADwMbPBXXIIN776YH5
e56O/AAEt53I6sXPA7w2nOQ4iuyOh/rrRfQu++up0wsWpypmontODc
GQgXKvARoFQHQQnoOdmO51jnkPkiYo9tl4OHITXp443psFNW1muLc0
gAEADKgkc0sUvxpwsY2U8M2b6g9TaVSP6ZXw3kHn2RVXZQ410Hkqd3
dD6iXtg3Vkur2j+Kt2syv2Dqle/n7vqPVxo97ZC7soTZ3W/hBsHwmq
SSPc3z3ePwz9db/6ZLve6nSglxP/sA8yQPEnw/hLWD2OLET1oeu7gz
Bw79xzzm0x7/tUUzbX1kVt2axurKzL9NU8oS+qzsO5xAsHXt/1veE/
nx4OQ3/cC92hFbg+t1piV9iCsqpAXFtrm6KF/5QGW8Kk5NptN1qwsy
nqO/db++iwO7Ab9qL2o8+3xT2SL+55/FhPuEF0PRQXrj7h+CmauQ9A
1LTRfBESCZvc53HQJjJ+tut/n09Ax8+1tmCiTR00CXBPB2eIK/WgTS
kUWtIXQdSHY+jQDi4t0U8bTwgc3COlljbWrJXamrW8sWFu1B8M3vvZ
0qq1vkrlZtVcukKd6zglRf+h2BQrgG3FrFZXV1INGpE38JGRG/ZcYn
HX+cT1r93c9N1R8HaB5sn9y9UVa215E+jj9iq+5b1vLy8ZtcBlV726
aa5NXz5P1RhdxObGxtKGubZaq168wrWIvCPaR1PETKtUfbul18Lepl
SVKzWCGV++IlscOKhyohN+gjpA7jzxgiAL3qeuvtFp2LXuwdLqhrA2
quviTtXcnBC+G8Yvie84FvESPoI+gdpj4C6/boEnknG79tKatb4myB
JrV12AuFTKzU1IxD2kFwhyGgYgyZnLjVNL8N10tbz57iJt06oub1ir
6xvmygZK482ksQfoAxBfohF/0dkDJDLEkKmpCYDLdwK1ADgP6oedT1
vcb1N4fYPgNFFev2yLg/rRXvsOtSz4smleoFP8Bl2KrrIHLbCuPUX3
cA+Tz3TtNr6JtpASe+D8pVzp89b4v5AssP0vKC5I9PjKaNDPSErA1M
cG7zuI5IxjejjBav8IRq1hgXzGyALVfd/D8SPhYcNdXqIhWqC7kGDW
hEndGaSMAl2Lajg2gE6LyGqJ2rtA2/4tbkDIoRTjUHmER+MRfRvC9v
gnMqVck3qsQlJ5EWpWFmzserRM3wbwG53VbbIJWcWPMLE3oOiAGLz7
1QV6WDiKGjb3WlIWXT8/wCQbDGMjDnmEbVb8R9yzB533P8JwK/4aan
sQF8XPiA4Vn1oZg+4ekXY145E1L9AFfmqYrYzx8hgrj7a28G30XYzu
jjCMXr/E67u4fvcfdK06D7XGiP01ocRJNMDl5z4MwQxo0pwEf+QLwu
1HUtODBLJc6oonbKmE/OZfsLGLJpbny5fkGAJpAFQvtwD4YQtivsSZ
ITmgQrJp6vwP+fHCevM/DQXsQDe8J1gHy6AVY45kkzsAP4eORF+k1fh
M/Udd+c21Q5avQOPSPoogSEnYEtyzYbVIkENLVzBoSuhYNXvlPRpSa
iCK3qeclxS8oguyIxJuvX0Y+tLlHxvyG4sBjh0UkbGtE5Iz/HSBCKd
Mj+YRt16gSfw08iMR/OZ8stMn2XRG/uqtr/0T+1aIK7faEDUjpRmPL
IipEAD7+AUH3lHYtAXGtMn0lVq4AlfIL0s8qGQw4BV2EJfrqcWYYhq
S4dUFG4ZCF89A1IkwS28hOjBeRfSOQKn55Ycuz0UeYNjF9eWkRAoRN
eUG5vhI8/xG2O8SMDyX58ITXIC7AaysaMQrxV/IEaUQIUGyeSX6P/F
0mynu+5HxEk5eXEELsG9xdJFTl6ZpNEL7C4ZFN32xs0yYC2AtS0u6W
/O0/LEccZyRuVKlVIiJojXPMJTnPjwy5k0gFIgT0VcSkRwNkKtOqTf
cZe7BpnqxdpGxyZhO4OFWTBlESINXM+BknoAoBo818g3MGASPRkh7y
+ND5hyBj/gmvPnn9kiD0H0oD/cdRha3DpjEpapbj59IPqcaWleQPyD
pFpq605ILN+oJ7ygLIQ0RCPnZGjylafL75B0dGkNQiZO1+wCxZ8myR
s50J/o3oMMXtahJx9PcfYGDQRgo0gyLQWrArRBPsXYAX51uU3rakw0
nqInsyEj0I2IHiM+F8XRAU3bO1eUmvfY3dFkcyLt43IFy3IM+55LzC2
6Y9hFAQUit5gJL+Nvwe4Fh+v0z0Q6N95KEhjSkLkdMvGV0Bd+zXhcH
vEjq/RX6jK2LsQIc7GDzFpf21Ij0myQVsaFAlMV/q6vEgRi40Orvdq
EqcIp8dlzyLewXqMbKKtTRMwRzxGjyjV4r1WpvxQ0pV/L7+Ov8eyya
nMQuJUu8JVbyjLG1YW+zw8JC5MqgCh3OzDr7+DLhO2eS3JP8C8c4uY
4s71Xcz5fcIRAwsrB2msXxiyQHhmJMGZ8+iV+QiV9x40fxdiVaLJvs
FewvAILw9JnQAvlfg76FG5tq+LfyR9/oXJ51Ow77UQgUeQ+HAX9312
bVuPKJtYVEM917KK5VUsqlg2VCSejOivzURgK/4CI4JoH8OKZRGAZv
wTbLuwIHKeAtCiC8nrv4Y9H28sGCuUjojblwo/Wm8dURz55ARMGRU6
/TnkjjyOiU93qd7A/H+EwedUcELOMCQHM/tIBETBL0gp4isqkHVpm5
b8O4vvj6iWLQvmoxlYBt/9WD8cuSIqdvw15t/zKpYYUf5F8FQufGH7
wv8cV3Gt1AS8hb6D8nMoQkrc3qMK/sEwX0TYQAkkovT/WYXIFH+BA/
OVBWHx68XnfMDzH9IW/KNg1P+MKR9a7xHvcQXFEAJNyWSVXFaZzSuF
jJLNK8U5RZ9RNLyXl8lVxaqSVXM5Rckp+bwyM6vMYamolHTlJu8v4A
MJOJVRcnSE0Obxjv341F1UpsxiD3YWeQOemMzyHp4vsfBCRs1mFAVL

FLS 186

DUW4g8nlFp5zyt+VeH90ØfMsJ6vMvZ2Ipb+qbfYttCI9nbY3WNwbrO
2vUmqVQMtVyUfWjD5bUmVzLJ9fsomSqqKRKGiWuaErtzIslJUssIb$
OWJuØVBV3leyO8rzHeVXmJFCoEmWMJfvM3i5obxT5u6CdRCL46A2Qd
MwhDwpzoWcUsC2Is/nlCJsxDNDGuGTlxBhCCgyKoQoqpqmp1KWijH+
hAZ2sua4bg7DIkMttVkTjXEoMghZ6T3pEZ5zyk1cLW2RVhRIgYzrr/
EVReCGnbOEnkt9hHl5HTTX2IkpbsWpYXaWPZLqmZ1CCcpkMkQh+jAs
uBfQ3ZzaQ4bOQXmF9JtRCBQqOEUtEXRqQTpuRs8zzchZ8uP5BMAMNz
1TUIuSHimmuOK0R1QaWfZI1kOWJ07MqyUWS2ikWsn9YDLgLaXMw4Xj
WeIPr3iDhLwKBDCcZbrmJPShIKGaqArbZ+mHL0XUWNEqORH6z0m/y7
toSc1NhVJBXopV1kebjgUiScIQwMUByEtsETbMMDwa85fkhsbBgtsp
xLAKfHRF8ZV38km4kKpMDIQnAYV3GRdyFU8pOabJsMX+G4xVgTgDHo
IkN65qadzNchzlDFoLCRuTe2+mSSChqApTpMtUCFQKZCPRmLUiu8Dd
a4ComoypLIeV1G2ygW5X5+QGzLMXMpyX8mmczmg0n2ePw18lhrfA4S
AlSHhpjvPYDaaMjJ00pmalgdL8mSQSk1wtI65AMa73/VgibqTBLFHs
F58YYN6CkkeA31RuMc7SQABVkGRgTGBAVrJCJcVXkP73ls45kxyhJt
uyYImMhFFqBDW5FE3bEqpwfsjcVN6RNJtiOHL7LU2Zy9HLTfmU2fuG
civHO+WHuQHvUBLIqsVZBVjMJjxUcxQU1YPgO514fk237BtGATPOQE
3EImyzan5KLCUHIoZaZFjgiRznxmxJmWXJPFSzMoFoMmNMBVHmKsGC
gTc5rVG6luYXeINkdUEt8RV5GV9ZN5Mw4sAh27ENEFF8qfkpc6S8+W
IHSGVKskFCIWNhlsmfT/177RY1N2UykIKIReqMNCeTIiapJStmhniY
JJOfPfEp8lt8yslMOIzS8280Ayvyqlpg Y3MyR3FeiTNJE17KJTYEZh
altAyTVqY1dnReGkszivFSZkFVNYIkhtqGrHxnAud5MscSE1WzJDaX
Dgt6I2HJWslTRR7mOdvPsL58KvHmvJiZViZhS15NihpAK8jrsskt KQ
IJVsUpuPI8zLOxhVRVWbK1BnKVyyYC6QqGRZNG8TA3AZCRmWBeSG9P
1MjI/Rgnt0s9YWAxaxh4pYluO522fCQIwQ7/GTYWcuakZJWymaR5I97
T9SHWBMyUzl7YfxR59CRoIRgmsPrl62vyUGLasIUMZtMfplVUzdJ10
RDH1l5yQSUGeSYVnr8iQ7CmKpb+UeG2iZIiPkwGNZRZgmXE4EZaU
vqxMQnn7kiHjazasJPKTCTnmGyp5jW9HxolyQMa3ILSV9IXa1O8eaU
zpzJ8yEZiYAvQ48Kd4Y1L6XcyGWc4c8cXMaILKVFuZSZzCehV+JEUU
pWE/BySSHsN0GAgpSPFydBuHZ1krhwp3IJgJPaudSD+Sn0C5krxApT
0EkCyFCS71hMcFavzedSX+cmsaNyP5N6Jzd1ZMpf+Um0TmNbfIpbMS
WJdAp7L2mUV0isZ1Xu6FKCFVKvJSgxI8PqzmRSLqVaFdOQnDB23mgj
e8XS7CQ78U6poTbJCTwju2jp4mzCig5N5R4orFTKrKGnsOe4fyuq/w N5uKaxeikAAA==
X-MS-Exchange-Forest-IndexAgent: 1 588I
X-MS-Exchange-Forest-EmailMessageHash: 00000000,8D7577BC
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 14 Jul 2023 13:15:51.6537
(UTC)
X-MS-Exchange-CrossTenant-Network-Message-Id: fa5ecd71-3443-4aee-354a-08db846c72ec
X-MS-Exchange-CrossTenant-Id: 23f845ec-3f64-4302-bf5d-2a67cf6c2472
X-MS-Exchange-CrossTenant-AuthSource:
DM3NAM02FT021.eop-nam02.prod.protection.outlook.com
X-MS-Exchange-CrossTenant-AuthAs: Anonymous
X-MS-Exchange-CrossTenant-FromEntityHeader: Internet
X-MS-Exchange-Transport-CrossTenantHeadersStamped: CPWP152MB5144
X-MS-Exchange-Organization-OutboundCrossTenantAgentProcessed: CPWP152MB5144
X-MS-Exchange-Organization-DelayAnalysis-Summary: Processed

FUNDAÇÃO DO ABC

Versão e Revisão:

Versão	Revisor	Data
1.0	Eduardo Nobuo Okada	28/07/2023
1.0	Gustavo Breder Dias	28/07/2023

São Bernardo do Campo, 28 de Julho de 2023

Eduardo Nobuo Okada

Coordenador de Suporte TI

Luis Henrique Camboraia Galvao

Gerente de TI

Dra. Agnes M. F. Ferrari
Diretora Geral
CHMSBC