MUNDINVEST S/A – CORRETORA DE CÂMBIO E VALORES MOBILIÁRIOS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA (PSIC)

A Mundinvest S/A – Corretora de Câmbio e Valores Mobiliários estabelece a seguinte **Política da Segurança da Informação e Cibernética**, que deverá ser praticada por todos os seus colaboradores, parceiros e prestadores de serviços.

Introdução: A segurança dos arquivos e dados da Corretora é de extrema importância para manter a confidencialidade, integridade e disponibilidade de suas informações.

O objetivo da **Política da Segurança da Informação e Cibernética** é apresentar um conjunto de instruções e procedimentos para normatizar, melhorar a visão e a atuação no quesito segurança da informação. As normas estabelecidas nesta **Política** deverão ser seguidas por todas as pessoas acima mencionadas.

Ao tomar conhecimento desta **Política** os colaboradores, parceiros e prestadores de serviços se comprometem a respeitar todas as regras abordadas pela mesma, estando cientes, por exemplo, de que seus e-mails e o conteúdo de sua navegação na internet poderão ser monitorados.

O não cumprimento da **Politica** poderá acarretar em sanções administrativas, podendo ocorrer a descontinuidade dos serviços dos colaboradores, parceiros ou prestadores de serviços, de acordo com a gravidade da ocorrência, respeitando sempre a legislação vigente e os contratos porventura celebrados.

Segurança da Informação e Cibernética

Podemos definir Risco Cibernético como "os potenciais resultados negativos associados aos ataques cibernéticos" Por sua vez, os ataques cibernéticos podem ser definidos como "tentativas de comprometer a confidencialidade, integridade e disponibilidade de dados ou sistemas tecnológicos."

As instituições financeiras devem se preocupar com a integridade de suas informações, mas sobretudo com as informações cadastrais de seus clientes, que são seu maior patrimônio.

Com os avanços tecnológicos, aqueles que querem levar vantagens indevidas criam cada vez mais meios de invadir bancos de dados com intenções de conseguir informações com as quais possam praticar atos ilícitos, prejudicando, sobretudo os clientes das instituições.

Por este motivo faz-se necessário que as instituições de modo geral e, as financeiras de modo específico, busquem ferramentas de maneira a proteger suas informações e de seus clientes, contra ataques de organizações criminosas, *hackers*, concorrentes, etc.

Desta forma a Mundinvest S/A – CCVM descreve a seguir as possíveis identificações de risco cibernético a que está sujeita, as ferramentas com as quais poderá monitorar estes ataques, as ações que deverão ser tomadas em caso de detecção de possíveis ataques e o plano de execução para tratamento dos mesmos.

Identificação / Avaliação de Riscos (Risk Assessment)

Para seu funcionamento a Corretora utiliza sistemas, servidores e estações de trabalho, sendo que estas ferramentas estão sujeitas a possíveis riscos cibernéticos.

Para acesso a estas ferramentas a Corretora estabeleceu regras de acesso, parâmetros de senha, obrigatoriedade de antivírus, Firewall, regras para acesso a sites, política de concessão e de administração de acesso, política de e-mail, ferramentas de monitoração, política de uso das estações de trabalho e política de backup de forma a orientar seus colaboradores e parceiros na utilização das ferramentas.

Para segurança das informações e dos bancos de dados existentes a Corretora contratou a empresa NTI Informática Ltda para administração e monitoramento das ferramentas de segurança. Nos casos de identificação de comportamentos anômalos na rede, as ferramentas estão parametrizadas para emitir alertas, que são enviados por e-mail à prestadora de serviços e ao Supervisor de Tecnologia da Informação da Corretora que juntos realizarão as devidas tratativas.

Todos os equipamentos que compõem o parque tecnológico da Mundinvest para seu funcionamento, incluindo estações de trabalho e servidores, estão devidamente protegidos pelas ferramentas: Firewall Sophos, antivírus Anti Ransomware Sophos, a fim de minimizar vulnerabilidades, exposições e possíveis impactos financeiros aos ativos operacionais e reputacionais da Corretora.

Além da contratação do prestador de serviços NTI Informática Ltda, a segurança da informação e cibernética é objeto de constante monitoramento das áreas de Tecnologia da Informação, Controles Internos e da diretoria de Tecnologia da Informação, que acompanham os processos necessários para o bom funcionamento dos serviços prestados pela Corretora.

Os processos de Tecnologia da Informação devem ser objetos constantes de auditoria interna e externa, bem como dos Órgãos Reguladores aos quais a Corretora está submetida.

Ações de Prevenção e Proteção

Política de Concessão e administração de acessos e Sistemas, à Base de Dados e a Rede: Os Diretores junto com o Proprietário da Informação realizarão o processo de aprovação, alteração e revogação de acessos aos sistemas e da Rede da Corretora junto a área de Tecnologia da Informação, sempre por meio de e-mails.

O Administrador da rede será o único autorizado a atribuir senhas de acesso ou efetivar o cancelamento de senhas para os demais funcionários e parceiros da Corretora.

O acesso será concedido de acordo com a Matriz de Segregação de Função aos Sistemas da Corretora, obedecendo-se aos seguintes critérios:

Conforme Matriz de Segregação de Função os acessos serão determinados considerando-se os Departamentos e os Sistemas utilizados na Corretora, contendo as seguintes permissões: sem acesso, acesso para consulta, acesso com poderes de edição e acesso administrativo.

Os acessos serão concedidos e/ou revogados mediante autorização expressa da Diretoria ou Proprietário da Informação da Corretora, podendo ser por escrito ou por e-mail enviado diretamente ao responsável pela área de Tecnologia da Informação, que ficará responsável pela concessão ou revogação dos acessos.

Os acessos aos sistemas e à rede serão feitos mediante *logins* e senhas estabelecidos para os colaboradores e parceiros da Corretora.

As chaves de acesso (LOGIN/LOGOF) da rede identificarão claramente seu detentor, na forma como ele é reconhecido na Corretora através da representação de seu nome.

As senhas serão alteradas no máximo a cada 90 (noventa dias) dias, de acordo com o critério definido pelo Parâmetro de senhas.

Tudo que for feito ou executado com a senha do colaborador, parceiro ou prestador de serviço será de responsabilidade do titular, devendo, portanto, o mesmo tomar todas as precauções necessárias para manter sua senha segura.

Política de Senhas: As senhas em hipótese alguma poderão ser transferidas para terceiros, pois é pessoal e intransferível. Caso o usuário desconfie que sua senha não esteja mais segura, deverá alterá-la imediatamente, mesmo antes do prazo determinado de validade.

É de inteira responsabilidade do usuário todo e qualquer prejuízo causado pelo fornecimento de sua senha pessoal a terceiros, independente do motivo.

Parâmetro de Senhas: As senhas deverão seguir os padrões de segurança adotado pela Corretora.

As senhas de acesso à rede e aos sistemas internos devem seguir, pelo menos, os seguintes parâmetros:

Tamanho mínimo: 6 (seis) caracteres (maiúsculo, minúsculo, número e carácter);
Tempo máximo de expiração: 90 (noventa) dias;
Quantidade máxima de tentativas antes do bloqueio: 3 (três);
Desbloqueio de senhas: apenas pelo administrador;
Histórico mínimo de senhas utilizadas: 6 (seis);
Criptografia: ativada.

Responsabilidade dos Usuários: A autenticação nos sistemas de informática será baseada em uma senha. Senhas como nome do usuário, combinações simples (abc123), substantivos (empresa, cadeira, mesa, Brasil), datas (01122011) e outros são extremamente fáceis de serem descobertas. A senha deverá ser criada de forma coerente, observando a Política de Senhas.

O acesso ao CPD da Corretora é restrito aos responsáveis pela área de Tecnologia da Informação, sendo controlada por meio de controle de acesso.

Os backups deverão ser efetuados de acordo com a Política de Backup definida pela Corretora.

Os sistemas utilizados pela Corretora deverão obedecer a Política de Gestão de Mudanças para alterações efetuadas nos sistemas.

Os contratos celebrados com prestadores de serviço deverão ter cláusulas de confidencialidade e de SLA.

Ferramentas de Segurança de Rede e Monitoramento: Com o objetivo de garantir a segurança de seu ambiente de rede, a Corretora contratou a prestadora de serviços NTI Informática Ltda para administração e monitoramento das ferramentas de segurança.

As ferramentas são compostas por:

Firewall Astaro Security Gateway (firewall, IPS e IDS), protegendo o tráfego de internet e de sua Rede interna, nos casos de identificação de ataques externos, estando configurado para emitir alertas via e-mail para a Prestadora de Serviços e para o responsável pela área de Tecnologia da Informação da Corretora.

As regras do Firewall são alteradas e revisadas pela equipe da NTI Informática Ltda, sob demanda da Corretora.

Serviços do Firewall:

Verificação do registro de falhas.
Administração de desempenho dos serviços interligados ao Servidor.
Aplicação de softwares básicos para correção de falhas de segurança.
Interpretação de mensagens de erro, com diagnostico de medidas para solução.
Avaliação e análise de conectividade entre protocolos de comunicação.
Administração de políticas de segurança.
Acompanhamento de intervenções de operadoras e fornecedores de tecnologia.
Execução de tarefas programadas.

Zabbix: Solução de monitoramento de redes, servidores e serviços, pensadas para monitorar a disponibilidade, experiência de usuário e qualidade de serviços.
A ferramenta de monitoramento de redes Zabbix oferece uma interface 100% Web para administração e exibição de dados fornecendo relatórios para evidencias de auditoria. Os alertas do sistema de monitoramento Zabbix são configurados para utilizar envio de alertas por e-mail.

Sophos Intercept X Advanced para Servidores: oferece proteção de Antivírus e contra ransomware. Inclui várias camadas de segurança que oferecem proteção contra ataques avançados e sofisticados.

Ações de Prevenção e Proteção: A tecnologia CryptoGuard impede a criptografia não autorizada de arquivos pelo ransomware, transferindo todos os arquivos afetados de volta ao seu estado original.

A proteção contra exploração impede que o ransomware use vulnerabilidades em produtos de software para se infiltrar e se espalhar pelas organizações.

O mecanismo Deep Learning usa aprendizado de máquina de ponta para identificar e bloquear ransomware antes de os mesmos serem executados.

É enviado e-mail de alerta para eventos encontrados.

Sophos Endpoint Protection: Oferece proteção de seus sistemas Windows contra malware e outras ameaças a endpoints.

A proteção de endpoints da Sophos integra tecnologias comprovadas, como a detecção de tráfego mal-intencionado com inteligência de ameaças em tempo real fornecida pelo SophosLabs, para ajudar a prevenir, detectar e remediar as ameaças facilmente.

Controle da Web que faz Filtragem da web por categoria, executada dentro e fora da rede corporativa.

Controle de aplicativos: Bloqueio de aplicativos por categoria e nome.

Controle de periféricos: Acesso gerenciado a mídias removíveis e dispositivos móveis.

Política de e-mail: O usuário nunca deverá abrir anexos de e-mails com arquivos de extensões .bat, .exe, .src, .lnk e .com (Ex: "Anexo.bat"; "Arquivo.exe"; "Foto.src"; "site.Ink" ou "portal.com") se não tiver certeza de que solicitou o referido email.

Não é recomendado abrir e-mails com assuntos estranhos e/ou em outras línguas, neste último, considerando exceção de setores com contatos estrangeiros.

Não encaminhar ou reenviar e-mails do tipo corrente, aviso de vírus, avisos da Microsoft / AOL / UOL / YAHOO / GOOGLE / GNU / Symantec, criança desaparecida, criança doente, pague menos em alguma coisa, não pague alguma coisa, "você ganhou alguma coisa", etc.

Não utilizar o e-mail da Corretora para assuntos pessoais;

Evitar o envio de e-mails para mais de 10 pessoas de uma única vez (to, cc, bcc);

Evitar anexos com tamanhos acima de 10MB.

Política de Acesso à Internet: O uso da internet deverá ser feito de forma responsável e somente para interesse de trabalho para a Corretora, podendo o usuário vir a prestar contas de seu mau uso.

O uso da internet para assuntos pessoais, e que possa acarretar problemas para Corretora, como sites de relacionamento e outros são proibidos.

São ainda proibidos: acessos a sites com conteúdo indevidos como pornografia, bate-papo, jogos, qualquer tipo de apostas e semelhantes; uso de ferramentas P2P de compartilhamento de arquivos (Ares Galaxy, LimeWire, kazaa, eMule, Torrent, etc); uso de IM (Instant Messengers) não homologados/autorizados pelo responsável pelo Departamento de Tecnologia da Informação da Corretora; download de qualquer arquivo que não tenha a finalidade de uso comercial ou que violem direitos autorais e a utilização de mecanismos que burlem o acesso a sites proibidos ou de acesso não desejado.

Política de uso de estações de trabalho: Cada estação de trabalho tem sua identificação na rede e qualquer usuário cadastrado terá acesso às pastas Públicas.

Isso significa que tudo que venha a ser executado em determinada estação de trabalho será de inteira responsabilidade do usuário que estava, no momento do fato, autenticado na estação.

Sendo assim, o usuário deverá tomar o cuidado de, ao sair de sua estação, verificar se efetuou *logoff* ou bloqueou a máquina, para evitar que pessoas estranhas tenham acesso à mesma.

Não é permitida a instalação de qualquer tipo de software em estações de trabalho sem autorização do responsável pela área de Tecnologia da Informação.

Não é permitido manter nas estações de trabalho softwares com direitos autorais sem terem sido adquiridos legalmente, ou qualquer outro tipo de pirataria.

Caso não saiba como proceder em qualquer das situações apresentadas acima, o usuário deverá entrar em contato com o responsável pelo Departamento de Tecnologia da Informação da Corretora informando o acontecido, para que sejam tomadas as devidas providências.

Política Social de Tecnologia da Informação: Em algumas situações, quando discorremos em nosso meio social sobre segurança, devemos observar os seguintes critérios: Não mencionar sobre a Política de Segurança da Informação da Corretora em locais públicos, ou ainda com terceiros; não informar a senha de autenticação para nenhuma pessoa.

O usuário somente deverá aceitar ajuda técnica do responsável pela área de Tecnologia da Informação tendo ciência de que o mesmo nunca enviará e-mail com procedimentos técnicos.

Os usuários deverão relatar aos responsáveis quaisquer pedidos externos ou internos que venham a discordar dos tópicos apresentados acima.

Portanto é obrigação do usuário relatar qualquer tipo de anormalidade que venha a ocorrer em sua estação de trabalho.

O usuário deverá reportar ao responsável pela área de Tecnologia da Informação qualquer atitude suspeita em sua estação de trabalho, para que possíveis vírus ou malwares possam ser identificados no menor espaço de tempo possível.

Somente pessoas autorizadas poderão acessar os ambientes de operações e processamento das informações.

Os colaboradores que utilizarem os sistemas CBLCnet e SINACOR deverão estar devidamente certificados pela B3 em suas respectivas áreas de atuação.

Monitoramentos e Testes

Monitoramento de segurança: A Corretora conta atualmente com a prestação de serviços do fornecedor NTI Informática Ltda, que nos disponibiliza as ferramentas Sophos Intercept X (anti ramsoware), Sophos Endpoint Protection, *firewall* Astaro Security Gateway (*Firewall*, IPS e IDS) e Zabbix (para monitoração contínua da capacidade e desempenho dos Servidores e Estações de Trabalho).

O monitoramento de segurança dos Servidores e estações de Trabalho na rede é realizado pelo Aplicativo de Antivírus Sophos Intercept X (anti ramsoware).

A segurança de entrada e saída de dados é realizada pela ferramenta de firewall Sophos, bloqueando acessos de portas não autorizadas.

A ferramenta de Firewall e antivírus estão configuradas para agir automaticamente. Em caso de ocorrência, a ferramenta envia alertas automaticamente para o Supervisor de Tecnologia da Informação e ao prestador de serviço NTI Informática Ltda para conhecimento do problema.

Após avaliação é aberto o chamado no sistema GTI, que envia e-mail para o supervisor de Tecnologia da Informação, para o e-mail cpd@mundinvest.com.br.

As tratativas serão executadas pelo prestador de serviço e ou supervisor de Tecnologia da Informação de acordo com as necessidades exigidas no momento.

Monitoramento da execução do *backup*: O monitoramento da execução dos backups é realizado por meio de análise dos logs da ferramenta Iperius Backup, que são gerados e enviados automaticamente para os e-mails do fornecedor Nattive e o supervisor de Tecnologia da Informação da Corretora. Os logs serão analisados pelos responsáveis, e em caso de identificação de falhas, será aberto chamado para realizar as devidas correções e reprocessamento do backup.

O Participante possui procedimento definido para realização de testes de *restore* e todos os testes são realizados e documentados pelo Supervisor de Tecnologia da Informação.

Monitoramento dos Servidores e Estações de trabalho: O Participante utiliza a ferramenta Zabbix para monitoração contínua da capacidade e desempenho de sua infraestrutura. Faz parte do escopo da monitoração os servidores (hardware) de banco de dados e dos sistemas do escopo da auditoria, sendo monitorados pelo menos os seguintes itens:

- Utilização do processamento (CPU);
- Utilização de Memória (RAM);
- Utilização de Capacidade de espaço em disco; e
- Disponibilidade (Uptime).

A monitoração é realizada pela ferramenta que é disponibilizada pelo fornecedor NTI Informática Ltda, estando a ferramenta parametrizada para emitir alertas por e-mail para a equipe da NTI Informática Ltda e ao Supervisor de Tecnologia da Informação da Corretora. Em caso de anormalidades o Supervisor de Tecnologia da Informação é o responsável por realizar as tratativas das ocorrências.

Atualização de segurança do sistema operacional (Windows): O processo de atualização das patches críticas e de segurança do Windows nas estações de trabalho e servidores do Participante, estão parametrizados para serem executadas automaticamente em horário que não possam interromper os trabalhos dos usuários.

Plano de Resposta

Caso as ferramentas detectem a tentativa de invasão que possa significar risco cibernético para a Corretora imediatamente serão disparados alertas informando o pessoal responsável pelo monitoramento, que tomarão as seguintes providências:

Caso a Corretora sofra algum tipo de ameaça em seus equipamentos as ferramentas de segurança emitirão alertas por e-mail para a Corretora e para o prestador de serviços NTI Informática Ltda para que, cientes do problema, tomem as providências necessárias para solução do mesmo.

Todo e qualquer incidente relevante que possam impactar os serviços prestados pela Corretora deve ser reportado imediatamente pela equipe de Tecnologia da Informação ao Diretor responsável pela área, devendo a equipe tomar as providências cabíveis para colocar em prática o plano de ação da Corretora para solução do incidente e normalização dos serviços prestados pela Instituição.

Reciclagem e revisão

Tendo em vista a rapidez com que as ameaças cibernéticas estão sendo aprimorada faz-se necessário que as atenções voltadas para segurança contra estes ataques sejam monitoradas diariamente, devendo todos os colaboradores da Corretora estarem atentos a qualquer fator que possa parecer risco para a Corretora, devendo o fato ser informado imediatamente para o responsável pela área de Tecnologia da Informação.

Esta Política deverá ser monitorada permanentemente, devendo ser revisada, no mínimo anualmente, sendo sua atualização aprovada em Ata pela Diretoria da Corretora.

A Política de Segurança da Informação e Cibernética deverá ser divulgada para todos os colaboradores, parceiros e prestadores de serviço da Corretora.

Belo Horizonte, 10 de novembro de 2021.

MUNDINVEST S/A – CORRETORA DE CAMBIO E VALORES MOBILIÁRIOS

Eduardo de Almeida Pinto
Diretor

João Carlos de Magalhães Lanza
Diretor

José Domingos Vieira Furtado
Diretor

Antonio Luzia Gomes
Diretor

MUNDINVEST
CORRETORA DE VALORES

CIENCIA DOS COLABORADORES

Declaro que li a Política de Segurança da Informação e Cibernética da Mundinvest S/A – CCVM tomando conhecimento de seu inteiro teor.

Carlos Alberto de Paula

Jacques Magalhães Silva Jeronymo

Marilene Buitrago

Rosanea Ferreira Guimarães

Sérgio Luiz de Magalhães Lanza

Lioni de Souza Diniz