POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – Global - Segurança da Informação

1 Sumário

1. Objetivo

Este documento tem como objetivo explicar e estabelecer os requisitos de segurança da informação da empresa para todos os colaboradores, prestadores de serviços e parceiros. A administração da Total Biotecnologia / Biotrop adotou esta política de segurança para proteger a informação com o objetivo de atingir suas metas comerciais ou de conformidade com normas e leis aplicáveis.

2. Classificação do documento e alvo

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que utilizam, mantêm ou lidam com ativos de informação da Total Biotecnologia / Biotrop.

3. Comitê de Segurança da Informação – PSI 03

O Comitê de Segurança da Informação tem por objetivo auxiliar na criação e revisão de políticas, normas e procedimentos gerais relacionados à segurança da informação.

É responsabilidade do Comitê garantir a segurança da informação, a preservação dos ativos, a garantia de execução dos processos minimizando e mitigando riscos à Total Biotecnologia / Biotrop.

O Comitê possui autonomia para debater e/ou recomendar quaisquer aspectos relacionados à segurança da informação, oferecendo subsídio à Diretoria no processo de tomada de decisão.

Caso haja necessidade, podem ser formadas comissões específicas para debater alterações dentro dos procedimentos contidos nesta política.

4. Responsabilidades dentro da Política de Segurança da Informação

4.1. Organizando a Segurança da Informação

Constitui-se nesta política a responsabilidade ao departamento de Tecnologia da Informação, conjuntamente com o Comitê de Segurança da Informação, de assegurar a seleção de controles de segurança adequados para proteger os ativos de informação e proporcionar confiança ao negócio onde a Total Biotecnologia / Biotrop atua.

4.2. Papeis e Responsabilidades da Segurança da Informação

4.2.1 Premissa de Segurança da Informação

A proteção bem-sucedida dos sistemas da Total Biotecnologia / Biotrop requer que vários departamentos e grupos sigam consistentemente uma visão compartilhada de segurança.

O Comitê de Segurança da Informação trabalhará com os gerentes, administradores e usuários de sistemas dos departamentos no desenvolvimento de políticas, normas e procedimentos de segurança para garantir a proteção dos ativos da Total Biotecnologia / Biotrop.

O Comitê de Segurança da Informação possui a responsabilidade sobre o planejamento, a educação e a conscientização sobre o tema da segurança da informação. As responsabilidades específicas do Comitê

de Segurança da Informação incluem:

Responsabilidades do Comitê de Segurança da Informação

- Criar políticas e procedimentos de segurança da informação quando necessário.
- Manter e atualizar políticas e procedimentos de segurança da informação existentes.
- Rever anualmente as políticas e auxiliar a administração com o processo de aprovação.
- Atuar proativamente para implantação das políticas de Segurança da Informação.
- Criar e manter procedimentos de resposta a incidentes.
- Restringir e monitorar o acesso a áreas restritas e informação confidencial.
- Assegurar que os controles adequados estejam disponíveis onde houver informações confidenciais.

4.2.2 Departamento de Recursos Humanos

Devido ao seu relacionamento direto e constante com os funcionários, assim como sua posição única de ter a primeiras e últimas interações com todos os colaboradores, o Departamento de Recursos Humanos tem um papel importante no que se refere à segurança das informações dentro da Total Biotecnologia / Biotrop. Onde não houver um departamento específico para sua atuação, o mais próximo deverá ser alocado, sendo os seguintes itens de sua responsabilidade:

Responsabilidades do Recursos Humanos

- Auxiliar o Comitê de Segurança da Informação com a publicação e divulgação das políticas de Segurança da Informação e orientação sobre o uso aceitável a todos os usuários de sistema relevantes incluindo prestadores de serviço.
- Trabalhar com o Comitê de Segurança da Informação na disseminação de informações de conscientização sobre segurança, utilizando diversos métodos de comunicação, de conscientização e educação dos funcionários (ex. pôsteres, cartas, memorandos, treinamento via web, reuniões etc.).
- Trabalhar com o Comitê de Segurança da Informação para administrar sanções e ações disciplinares referentes a violações da Política de segurança da informação.
- Notificar o Departamento de Tecnologia da Informação quando qualquer funcionário for contratado ou desligado.

4.2.3 Usuários

Todos os usuários de recursos computacionais e de informação da Total Biotecnologia / Biotrop devem estar cientes da importância fundamental de tais recursos e reconhecer sua responsabilidade pela manutenção segura deles. Os usuários devem protegê-los contra abusos que interrompam ou ameacem a viabilidade de todos os sistemas. As seguintes responsabilidades são específicas a todos os usuários de sistemas computacionais da Total Biotecnologia / Biotrop:

Responsabilidades dos Usuários

- Entender as consequências de suas ações relacionadas às práticas de segurança computacional e agir de forma condizente. Aceitar a filosofia de que “Segurança é responsabilidade de todos" auxiliando a Total Biotecnologia / Biotrop a garantir a preservação de seus ativos e sistemas.
- Manter-se cientes sobre o conteúdo das políticas de Segurança da Informação.
- Ler e assinar o termo de responsabilidade referente as informações contidas na Política de Segurança da Informação.
- Agir constantemente de forma a seguir as classificações de confidencialidade dos ativos de informação da Total Biotecnologia / Biotrop.

4.3. Segregação de Funções

Para todos os ambientes da Total Biotecnologia / Biotrop, sejam eles de produção ou desenvolvimento, é obrigatória a implementação de segregação de funções. A segregação de funções determina que funções conflitantes e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação não autorizada, coibindo o mau uso dos ativos da Total Biotecnologia / Biotrop intencional ou não intencional. Para casos de exceção, seja por limitação técnica ou de negócio, é obrigatório o uso de controles adicionais de segurança e a aprovação do Departamento de Tecnologia da Informação.

4.4. Contato com as Autoridades Externas

Como parte do processo de comunicação interno e externo e do plano de resposta a incidentes de segurança da informação da Total Biotecnologia / Biotrop, declara-se que qualquer comunicação relacionada à segurança da informação, junto às autoridades externas que incluem, mas não se limitam a entidades reguladoras, entidades de conformidade e governo, devem ser previamente autorizadas pela Diretoria.

4.5. Segurança da Informação no Gerenciamento de Projetos

Como parte da metodologia de gerenciamento de projetos da Total Biotecnologia / Biotrop, recomenda-se que os projetos incluam a segurança da informação dentro do seu ciclo de vida. A inclusão tem como objetivo avaliar os riscos de segurança da informação, bem como propor controles adequados e acrescentar aos objetivos do projeto, aspectos de segurança de informação.

4.6. Conformidade Legal

Todos os ativos e sistemas de informação da Total Biotecnologia / Biotrop, assim como os seus funcionários e prestadores de serviço devem estar em conformidade com as obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação estabelecido pela Total Biotecnologia / Biotrop.

Com objetivo de prevenir violações, todas as informações armazenadas ou que trafeguem dentro dos perímetros físicos e lógicos da Total Biotecnologia / Biotrop podem ser monitoradas, mediante o processo de aprovação instituído, revisado pelo Comitê de Segurança da Informação. Violações não serão toleradas e as sanções apropriadas serão aplicadas.

5. Seções da Política de Segurança da Informação

5.1. Política de Gestão de Ativos

Todos os ativos físicos e de informação da Total Biotecnologia / Biotrop deverão ser classificados de acordo com o seu nível de confidencialidade, disponibilidade, integridade e controles legais. Uma vez classificados, devem ser respectivamente relacionados ao modo como são acessados, armazenados, movimentados e por fim descartados.

5.2. Política de Controle de Acesso

Todos os sistemas de informação da Total Biotecnologia / Biotrop devem estar integrados a um sistema de controle de acesso definido pelo Departamento de Tecnologia da Informação.

A concessão de acessos (recursos ou sistemas) deve ser aprovada pelo gestor da informação. Além disso, deve ser instituída a segregação de função de acordo com nível funcional ou responsabilidade assim como uma revisão periódica dos acessos concedidos, a fim de evitar acessos indevidos.

5.3. Política de Criptografia

Quando pertinente, as informações da Total Biotecnologia / Biotrop ou de parceiros e clientes que precisem ser protegidas contra acesso não autorizado ou estabelecido por normas externas ou internas de conformidade devem ser criptografadas conforme os padrões alinhados e definidos entre o responsável pela informação e seu detentor, de modo a garantir sua a confidencialidade, autenticidade e integridade.

5.4. Política de Segurança Física e do Ambiente

É necessário estabelecer o perímetro de segurança física de modo a preservar o acesso somente a pessoas autorizadas. Além disso, deve ser instituído de modo obrigatório o uso de identificação visual para visitantes, clientes, fornecedores e prestadores de serviço. Para controle e liberação de acesso de colaboradores, deve-se utilizar sistema de registro de acesso físico por meio de sistemas de catracas e biometria quando possível.

5.5. Política de Gestão de Operações

O Departamento de Tecnologia da Informação, conjuntamente com o Comitê de Segurança da Informação, deve estabelecer as diretrizes para garantir a operação segura e correta dos recursos de processamento da informação. Para isso deve estabelecer procedimentos operacionais documentados e acessíveis aos usuários necessários.

Estes procedimentos operacionais devem incluir e não se limitar a procedimentos de instalação e configuração de sistemas, procedimentos para manipulação de informação, procedimentos de cópias de segurança (backup) e procedimentos para gerenciamento de falhas de produção.

5.6. Política de Segurança nas Comunicações

O Departamento de Tecnologia da Informação, conjuntamente com o Comitê de Segurança da Informação, deve estabelecer as diretrizes para garantir a proteção das informações em redes e dos recursos de processamento da informação que as apoiam. Para isso deve estabelecer procedimentos operacionais documentados e acessíveis aos usuários necessários, que estabeleçam as responsabilidades e procedimentos sobre o gerenciamento de equipamentos de rede.

5.7. Política de Gestão de Sistemas da Informação e Infraestrutura

Todos os processos que envolvam aquisição, desenvolvimento ou manutenção de sistemas de informação ou alteração na infraestrutura da Total Biotecnologia / Biotrop devem ser comunicados ao Departamento de Tecnologia da Informação, garantindo que os riscos relacionados sejam conhecidos e tratados.

5.8. Política de Gestão de Incidentes de Segurança da Informação

O processo de gestão de incidentes de segurança da informação tem como objetivo garantir que eventos de segurança da informação associados a ativos de informação da Total Biotecnologia / Biotrop sejam comunicados ao Departamento de Tecnologia da Informação.

É de responsabilidade do Departamento de Tecnologia da Informação coordenar todas as atividades pertinentes ao processo de gestão de incidentes de segurança da informação. É dever de todos os usuários comunicar um incidente de segurança da informação para a área responsável.

5.9. Política de Mesa e Tela Limpa

A política de mesa limpa e tela limpa se refere a práticas relacionadas a assegurar que informações sensíveis, tanto em formato digital quanto físico, e ativos (e.g., notebooks, celulares, tablets, etc.) não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso,

ou quando alguém deixa sua área de trabalho, seja por um curto período de tempo ou ao final do dia.

5.10. Política de Dispositivos Móveis

Uma política de segurança para dispositivos móveis é um conjunto de medidas emitidas pela Total Biotecnologia / Biotrop para garantir que todos os usuários de suas redes cumpram as regras relacionadas à segurança das informações armazenadas e processadas digitalmente.

5.11. Política de Trabalho Remoto

Uma política de trabalho remoto é um conjunto de diretrizes e limites que descreve como e quando os funcionários podem trabalhar em casa ou em qualquer outro local remoto. Essa política de trabalho remoto comunica as melhores práticas a serem seguidas, que ajudam a empresa a manter a ordem e estabelecer expectativas claras.

6. Regulamentos Externos

ISO 27000 / ISO 27001 / ISO 27002

7. PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: SEGURANÇA NAS COMUNICAÇÕES

1. Objetivo

Este documento tem como objetivo destacar a importância da comunicação como um processo estratégico de gestão que permeia todas as ações da empresa.

Sistematizar todas as ações, produtos, fluxos e processos de comunicação em vigor ou a serem implementados na Total Biotecnologia / Biotrop, tendo em vista incrementar e qualificar a interação com os seus respectivos públicos.

Padronizar diretrizes, condutas, posturas, valores e princípios de modo a garantir coerência e eficácia no processo de comunicação interno e externo.

2. Descrição

2.1 Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que mantêm negócios com a Total Biotecnologia / Biotrop.

2.2 Seções da política e responsabilidades

2.2.1 Processo de Comunicação

Toda a comunicação interna e externa da Total Biotecnologia / Biotrop deve ser realizada seguindo as seguintes diretrizes:

Clareza: As informações devem ser passadas de maneira clara evitando duplo sentido;

Formalidade: Toda a comunicação deve ocorrer de maneira formal e profissional;

Objetividade: Para o efetivo processo de comunicação, não devem ser abordados assuntos distintos no mesmo meio de comunicação ao mesmo tempo;

Relevância: As informações só devem ser repassadas às partes que estão diretamente relacionadas ao conteúdo da mensagem;

Sensibilidade: As informações devem ser ajustadas para garantir que os interlocutores do processo obtenham o mesmo grau de entendimento sobre o respectivo assunto.

A comunicação Institucional externa deve ser realizada e/ou aprovada pelo departamento responsável com ciência da Diretoria.

2.2.2 Mensagens Eletrônicas

Para o uso adequado das ferramentas eletrônicas da Total Biotecnologia / Biotrop, todos os funcionários devem seguir as orientações abaixo:

Todos os Sistemas de Comunicação Eletrônica utilizados nas operações da Total Biotecnologia / Biotrop

são de propriedade da mesma, bem como todas as mensagens neles armazenadas para uso corporativo.

As mensagens devem ser limitadas apenas às necessidades da operação dos negócios da Total Biotecnologia / Biotrop.

O conteúdo das mensagens não pode possuir elementos que possam ser considerados ofensivos, destrutivos, difamatórios ou pejorativos, incluindo, mas não limitado a comentários ou imagens sexuais, calúnias raciais, ou outros comentários ou imagens que possam ofender a alguém por sua raça, nacionalidade, gênero, orientação sexual, crença religiosa, orientação política ou restrição física.

2.2.3 Direitos de Propriedade

É proibido carregar ou descarregar de sistemas internos ou de terceiros, material sujeito às leis de direito autoral ou classificados como confidenciais, sem autorização escrita por parte da Total Biotecnologia / Biotrop.

Materiais sujeitos às leis de direito autoral, classificados como shareware ou freeware podem ser utilizados para os propósitos designados pelo detentor do respectivo direito autoral.

2.2.4 Direito de Privacidade

Caso não seja diretamente mencionado, não se deve assumir que qualquer mensagem seja privativa. Apesar da característica dos sistemas darem uma aparência de privacidade, incluindo senhas e a possibilidade de se apagar as mensagens, não sendo necessariamente privativas por duas razões: os Sistemas de Comunicação Eletrônica podem não ser seguros, pois a segurança dos arquivos eletrônicos de sistemas compartilhados em redes é, frequentemente, semelhante ao de um documento em um envelope não lacrado, geralmente respeitado, porém facilmente lido por alguém determinado a fazê-lo. Deve-se assumir que as mensagens podem ser ouvidas ou lidas por alguém que não seja o destinatário. Mesmo quando uma mensagem é apagada, esta ainda pode ter uma cópia de segurança (backup) em algum lugar, ou é passível de ser recuperada.

As mensagens podem ser auditadas pela Total Biotecnologia / Biotrop a qualquer momento conforme as diretrizes de monitoramento descritas nesta política.

2.2.5 Direito de Monitoramento

A Total Biotecnologia / Biotrop se reserva ao direito de monitorar, acessar, recuperar e ler todas as mensagens, divulgando qualquer uma para as autoridades judiciais e policiais e terceiros caso considere necessário, sem aviso prévio ao remetente ou destinatário da mensagem.

Funcionários que têm sob sua responsabilidade profissional a integridade e segurança de dados podem revisar as mensagens recebidas ou enviadas por qualquer funcionário, desde que para os seguintes propósitos:

- Identificar e diagnosticar problemas de hardware ou software;
- Evitar má utilização dos sistemas;
- Determinar se houve violação de confidencialidade, segurança ou violação desta política;
- Investigar má conduta ou atividades não éticas, ilegais ou não apropriadas;
- Garantir o cumprimento dos direitos autorais, obrigações contratuais e licenças;
- Cumprir com as obrigações legais às quais a empresa está sujeita;
- Cumprir as requisições legais e regulamentadas de informações e proteger os interesses comerciais da Total Biotecnologia / Biotrop.

Nenhum outro tipo de monitoramento ou revisão pode ser feita sem a prévia aprovação da Diretoria da Total Biotecnologia / Biotrop.

2.2.6 Boas Práticas de Comunicação

A empresa não autoriza a utilização de mensagens eletrônicas com as seguintes descrições:

- Linguagem que possa ser considerada ofensiva, destrutiva, difamatória ou pejorativa.
- Para fins pessoais (mensagens para amigos e familiares, cadastro em site da internet, passar mensagens a outros funcionários que não sejam relacionadas ao trabalho).
- Manter nos computadores da Total Biotecnologia / Biotrop cópias ou instalação de programas que não sejam licenciados e que não estejam relacionados com os negócios.
- Divulgação ou compartilhamento de senha e/ou identificação de usuário com outras pessoas.
- Deixar seu computador sem supervisão quando estiver acessando a rede.

2.2.7 Falhas de Comunicação

Caso o funcionário receba mensagens eletrônicas com conteúdo que não esteja relacionado à sua atividade, deverá deletá-la e notificar à pessoa que enviou a mensagem sobre o erro.

Caso a pessoa insista em enviar mensagens de conteúdo inadequado, o funcionário deverá comunicar ao seu gestor sobre o problema para que as providências sejam tomadas. O uso indevido do Sistema de Comunicação Eletrônica pode resultar em ação disciplinar, incluindo dispensa. O código de ética da Total Biotecnologia / Biotrop deve mencionar as normas sobre a utilização de mensagens eletrônicas e dos recursos eletrônicos. Não é permitida a configuração de qualquer e-mail diferente do domínio da empresa nos computadores da Total Biotecnologia / Biotrop.

8. PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: CONTROLE DE ACESSO

1.Objetivo

Este documento tem como objetivo explicar e estabelecer os requisitos de segurança da informação relacionados ao controle de acesso dos colaboradores e prestadores de serviço que utilizam as redes da Total Biotecnologia / Biotrop.

A administração da Total Biotecnologia / Biotrop adotou esta política para assegurar que todos os colaboradores, prestadores de serviço, fornecedores e outros parceiros estejam cientes dos seus papéis e responsabilidades em relação às permissões de acesso dentro da Total Biotecnologia / Biotrop.

2. Definições e abreviaturas

TI – Tecnologia da Informação

3. Descrição

3.1. Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que possuem acesso às redes internas da Total Biotecnologia / Biotrop.

3.2 Seções da política e responsabilidades

3.2.1 Gestão de Contas

Todos os colaboradores que necessitam de um acesso à rede interna da Total Biotecnologia / Biotrop possuem uma conta com determinado nível de acesso vinculado ao departamento no qual estão inseridos. Esta conta é utilizada para acessar os compartilhamentos e *softwares* relacionados com a sua rotina de trabalho.

Todos os colaboradores que possuem contas recebem acesso a um e-mail corporativo que será utilizado para comunicação interna e externa a serviço da Total Biotecnologia / Biotrop.

Toda conta de usuário dentro ambiente da Total Biotecnologia / Biotrop está inclusa em uma unidade organizacional (*Organizational Unit*) que possui regras de acesso e direitos departamentais aos volumes compartilhados na rede, que por sua vez estão dentro das regras de acesso e direitos gerais do domínio da empresa.

3.2.2 Liberação de direito de acesso

Após o processo de seleção e contratação de novos colaboradores, o departamento de Recursos Humanos ou departamento responsável, encaminhará um e-mail ao Departamento de TI, no qual solicita a liberação de acessos e ativos necessários para o exercício de suas funções profissionais.

3.3 Revogação de direito de acesso

Durante o processo de desligamento dos colaboradores, o departamento de Recursos Humanos ou

departamento responsável encaminhará um e-mail ao Departamento de TI, no qual solicita a revogação de acessos e devolução de ativos utilizados durante exercício de suas funções profissionais.

3.3.1 Alteração de direitos e acesso

Os acessos às informações e aos recursos de processamento da informação são liberados, alterados ou revogados conforme a solicitação da gerência ou responsável pelo departamento. Nas ocorrências em que o acesso às informações solicitadas pertencer a outro departamento, o gerente ou responsável pela informação deve também autorizar, alterar, revogar ou impedir o acesso. Toda solicitação deve ser formalizada por e-mail direcionado ao endereço do departamento de TI.

3.3.2 Liberação de acessos temporários

Em função da necessidade de acesso às redes internas da Total Biotecnologia / Biotrop para a execução de trabalhos ou prestação de serviços específicos, o departamento de TI deverá disponibilizar uma conta de acesso temporário. Este acesso pode ser encerrado ou prorrogado mediante identificação de necessidade pelo departamento requisitante em função da atividade desenvolvida.

3.4 Gerenciamento de Usuário e Senha

O Departamento de TI é responsável por manter as diretrizes de senhas nos computadores, servidores e sistemas. Também é responsável por orientar os usuários no cadastramento de novas senhas.

A senha é de responsabilidade do usuário, de uso pessoal e intransferível, não sendo permitido o seu compartilhamento. A mesma poderá ser alterada a qualquer momento ou caso seja identificada uma falha de segurança.

Caso o usuário necessite de auxílio para alterar a senha, o Departamento de TI deve ser acionado. Na ocorrência de algum usuário identificar que outro usuário esteja compartilhando a senha, o mesmo deve comunicar por e-mail ao Departamento de TI. Não é permitido o uso e cadastro de usuário genérico ou padrão para acesso à internet, a rede e a sistemas.

A construção da senha do usuário deverá ser realizada seguindo as seguintes recomendações:

- Comprimento mínimo de 8 caracteres;
- Possuir 2 caracteres maiúsculos, 2 caracteres minúsculos, 2 caracteres especiais e 2 números;
- Diferir das 6 últimas senhas utilizadas;
- As senhas deverão ser trocadas a cada 180 dias;
- Utilizar senhas de fácil memorização.

3.5 Requisição e devolução de ativos

Os ativos de informática da Total Biotecnologia / Biotrop devem ser solicitados através de um e-mail pela gerência ou responsável do departamento, direcionado ao Departamento de TI. A devolução dos ativos de informática ocorre nos casos de quebra, descontinuidade do ativo, alteração de função, desligamento do funcionário ou encerramento de contrato de fornecedor ou prestador de serviço. Em caso de desligamento do funcionário, o Departamento de TI deve ser informado pela gerência ou responsável do departamento de Recursos Humanos ou outro responsável através de um e-mail para solicitar quais ativos devem ser devolvidos.

3.6 Termo de Confidencialidade

Todos os funcionários devem assinar o documento “Termo de Confidencialidade e Responsabilidade” fornecido pelo Departamento de Recursos Humanos no ato da contratação. Nos contratos de clientes e fornecedores

firmados com a Total Biotecnologia / Biotrop deve obrigatoriamente constar uma cláusula de confidencialidade. Todos os contratos devem ser validados pelo departamento jurídico da Total Biotecnologia / Biotrop.

9. PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: CRIPTOGRAFIA

1.Tratativa

Anexo PSI 02_Política de Criptografia - Total Biotecnologia Biotrop.

10. PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: IDENTIFICAÇÃO DE ATIVOS

1. Objetivo

Este documento tem como objetivo explicar e estabelecer os requisitos de segurança para: identificar os ativos, sejam físicos ou lógicos da empresa e definir as devidas responsabilidades pela gestão deles. Esta política também visa assegurar que as informações recebam um nível adequado de proteção de acordo com sua importância para a Total Biotecnologia / Biotrop

2. Definições e abreviaturas

TI – Tecnologia da Informação

3. Descrição

3.1 Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço, fornecedores e parceiros que utilizam, mantêm ou lidam com ativos de informação da Total Biotecnologia / Biotrop. Exceções da política serão permitidas somente quando aprovadas antecipadamente por escrito pelo Departamento de TI.

3.2 Responsabilidade pelos ativos

3.2.1 Inventário dos Ativos

A Total Biotecnologia / Biotrop, por meio do Departamento de TI, tem a responsabilidade de gerir o inventário dos ativos da mesma.

3.2.2 Uso responsável dos ativos

O Departamento de TI é responsável pelos ativos em questão e têm a responsabilidade de estabelecer, por meio desta política, as diretrizes do seu uso responsável visando à proteção e manutenção dos mesmos.

- Ativos físicos
- Manter a preservação dos ativos;
- Comunicar o Departamento de TI imediatamente após o extravio, perda, furto, roubo, dano para garantir que as providências cabíveis sejam tomadas;
- Comunicar o Departamento de TI sobre qualquer tipo de comportamento incomum que pode ser causado pela contaminação do dispositivo por um vírus ou agente externo.
- Ativos de Informação
- Assegurar a proteção e sigilo das informações confiadas em função das atividades exercidas;
- Comunicar o Departamento de TI imediatamente após o extravio, perda, furto, roubo, dano para garantir que as providências cabíveis sejam tomadas;

- Caso o ativo seja utilizado em algum dispositivo eletrônico, o mesmo deve ser mantido com a tela bloqueada na ausência do usuário;
- Não é recomendado salvar nenhum ativo na área de trabalho. O usuário deve salvar o ativo em um compartilhamento da rede, devidamente protegida pelos sistemas de segurança descritos na Política de Segurança de Informação.

3.2.3 Devolução de Ativos

- O Departamento de TI, com suporte da área de Recursos Humanos ou departamento relacionado, tem a responsabilidade de estabelecer um processo que defina as diretrizes/controles para assegurar que todos os colaboradores, prestadores de serviço, fornecedores ou parceiros, devolvam os ativos da Total Biotecnologia / Biotrop, após o encerramento de suas atividades, do contrato ou do acordo.
- Para casos de uso de ativos pessoais (ou que não pertençam a Total Biotecnologia / Biotrop) utilizados em atividades da Total Biotecnologia / Biotrop, o Departamento de TI tem a responsabilidade de assegurar em seus processos que o conteúdo de direito da Total Biotecnologia / Biotrop, seja transferido para um local apropriado e em seguida removido de modo seguro e permanente do dispositivo.

3.3 Classificação da informação

- Todos os ativos de informação da Total Biotecnologia / Biotrop devem receber uma classificação, sendo responsável por esta tarefa o gestor da área. A classificação deve levar em consideração o seu valor, requisitos legais, sensibilidade e criticidade para a Total Biotecnologia / Biotrop. A classificação precisa estar visível e de fácil identificação.
- O gestor da área deve classificar toda informação e deve reavaliá-la logo após a sua alteração. Esta reavaliação deve ser feita embasada nos critérios descritos acima, sempre que o responsável ou a diretoria considerarem necessário.
- Os ativos de informação na Total Biotecnologia / Biotrop devem ser classificados conforme a matriz abaixo:

Classificação	Definição
Pública	Aplica-se a todas as informações que podem ser divulgadas interna ou externamente a Total Biotecnologia / Biotrop. A divulgação não autorizada não deve impactar séria ou negativamente a Total Biotecnologia / Biotrop.
Uso Interno	Aplica-se a todas as informações que podem ser divulgadas internamente a Total Biotecnologia / Biotrop. A sua divulgação externa não autorizada pode afetar negativamente a Total Biotecnologia / Biotrop e/ou seus funcionários.
Confidencial	Aplicam-se as informações comerciais, sensíveis e informações de clientes utilizadas estritamente dentro da Total Biotecnologia / Biotrop. A divulgação não autorizada pode impactar séria ou negativamente a Total Biotecnologia / Biotrop, parceiros de negócio e/ou seus clientes.

- Informações que não se enquadram em nenhum dos itens acima devem ser classificadas como CONFIDENCIAL e devem, portanto, ter os mesmos controles de acesso.

3.3.1 Rótulos e tratamento da informação

- Todos os ativos (físico ou de informação) da Total Biotecnologia / Biotrop e/ou de terceiros devem receber uma classificação e devem ser rotulados quando pertinente. A rotulagem deve refletir o esquema de

classificação estabelecido. Todo arquivo de terceiros é considerado CONFIDENCIAL e deve receber tratativa adequada.

- O Departamento de TI tem a responsabilidade de estabelecer um processo que defina as diretrizes/controles para assegurar a rotulagem dos ativos de informação da Total Biotecnologia / Biotrop e/ou de terceiros. Este processo deve ser de conhecimento de todos aqueles que se utilizam dessas informações.

3.3.2 Tratamento dos ativos

- Objetivando assegurar a proteção de acesso adequado para cada classificação de ativos de informação, definem-se as diretrizes para acesso, processamento, armazenamento e transmissão, conforme matriz abaixo:

Classificação	
	PÚBLICA
Acessada	▪ Sem restrição de acesso.
Armazenada	▪ Sem restrição para armazenamento.
Transmitida	▪ Sem restrição para transmissão, desde que autorizado, pelo gestor responsável pela informação.

Classificação	
	USO INTERNO
Acessada	▪ Deve haver um controle de acesso baseado em permissões de grupo/usuário. ▪ Deve haver um controle de acesso que permita apenas acesso interno.
Armazenada	▪ Deve ser armazenada apenas em ambientes internos da Total Biotecnologia / Biotrop. ▪ Exceções, devem ser autorizadas pelo Departamento de TI.
Transmitida	▪ Deve ser transmitida apenas em ambientes internos da Total Biotecnologia / Biotrop. ▪ Exceções, devem ser autorizadas pelo gestor da informação.

Classificação	
	CONFIDENCIAL
Acessada	▪ Deve haver um controle de acesso baseado em permissões de usuário. ▪ Deve haver um controle de acesso que permita apenas acesso interno.
Armazenada	▪ Deve ser armazenada apenas em ambientes internos da Total Biotecnologia / Biotrop. ▪ Deve ser armazenada de modo seguro (criptografado ou outro método existente), quando requisitado pelo cliente. *Consultar a Política de Criptografia* para mais informações.
Transmitida	▪ Deve ser transmitida apenas em ambientes internos da Total Biotecnologia / Biotrop ▪ Deve ser transmitido de modo seguro (criptografado ou outro método existente), quando requisitado pelo cliente. *Consultar a Política de Criptografia* para mais informações.

É recomendado que todo ativo de informação seja enviado ou entregue por um sistema de comunicação seguro ou por outro método de entrega que possa ser precisamente rastreado e que tenha sido aprovado pelo Departamento de TI.

3.4 Tratamento de mídias

3.4.1 Mídias impressas

- Materiais impressos contendo informações CONFIDENCIAIS devem ser protegidos por controles de acesso físicos apropriados conforme descrito nesta política.
- Relatórios impressos contendo informações CONFIDENCIAIS devem ser mantidos, armazenados ou arquivados fisicamente somente dentro de instalações seguras da Total Biotecnologia / Biotrop, e somente pelo tempo mínimo considerado necessário pelo terceiro e/ou responsável pela informação.
- Sob nenhuma circunstância os materiais impressos contendo informações CONFIDENCIAIS devem ser removidos de qualquer instalação da Total Biotecnologia / Biotrop sem prévia autorização do responsável pela informação.
- Toda mídia impressa contendo informações CONFIDENCIAIS devem ser armazenadas em um local seguro.
- Todo material finalizado contendo informações CONFIDENCIAIS deixam de ser responsabilidade da Total Biotecnologia / Biotrop no momento que são retirados da Total Biotecnologia / Biotrop. Caso seja necessária alguma exceção a esta regra, é de responsabilidade do gestor responsável pela informação avaliar e autorizar os impactos desta operação.

3.4.2 Mídias Eletrônicas

- Informações CONFIDENCIAIS não devem ser em nenhum momento copiadas em mídias removíveis, quaisquer sejam elas.
- Mídias eletrônicas contendo informações CONFIDENCIAIS de terceiros podem ser admitidas dentro do ambiente da Total Biotecnologia / Biotrop apenas para recepção de dados. A informação é, então, incorporada dentro das redes seguras e a mídia é devolvida ao terceiro ou destruída.

3.4.3 Mídias em trânsito

O uso de mídias físicas para transferência de arquivos só deve ser utilizado em caráter de exceção, pois o procedimento padrão deverá ser a utilização da troca de arquivos online via FTP (File Transfer Protocol) ou qualquer outro sistema seguro utilizado. Somente nos casos explicitamente solicitados, deverão ser utilizadas mídias físicas.

Toda mídia deve ser embalada e transportada de maneira segura de forma que o acesso não autorizado seja inibido.

Os arquivos preferencialmente devem ser gravados em mídias que não possibilitem alterações ou limpeza dos dados. Quando necessário, os arquivos deverão conter bloqueios por senhas.

3.4.4 Descarte de mídias

- O Departamento de TI tem a responsabilidade de estabelecer um processo, nesta política, que defina as diretrizes/controles para descarte de mídias de acordo com a matriz de classificação de ativos.
- Antes do equipamento de informática ou comunicação ser enviado a um fornecedor para troca, manutenção ou descarte, todas as informações confidenciais devem ser destruídas ou removidas de acordo com métodos aprovados contidos nesta política.
- Mídias removíveis de armazenamento de dados não podem ser doados para caridade ou de outra forma reciclados.

3.4.5 Descarte de Materiais Impressos

- Departamento de TI tem a responsabilidade de estabelecer um processo, nesta política, que defina as diretrizes/controles para descarte e destruição de materiais impressos de acordo com a matriz de classificação de ativos.
- Recipientes usados para armazenamento de mídias a serem destruídas (como recipientes que contenham papel a ser fragmentado) devem ser armazenados em local controlado para evitar o acesso ao seu conteúdo antes do processo de destruição.
- Registro das destruições de material físico deve ser mantido pelo departamento de TI por meio de uma planilha eletrônica.

11. PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1. Objetivo

Assegurar que os eventos de segurança da informação sejam tratados de forma efetiva, permitindo o registro, investigação e tomada de ação corretiva adequados e em tempo hábil para mitigar os impactos sobre os sistemas de informação da empresa.

2. Definições e abreviaturas

TI – Tecnologia da Informação

3. Descrição

3.1 Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que utilizam, mantêm ou lidam com ativos de informação da Total Biotecnologia / Biotrop.

3.2 Seções da política e responsabilidades

3.2.1 Funções e Responsabilidades

É responsabilidade de qualquer integrante do Departamento de TI quando identificar um incidente, notificar os demais membros da equipe para que as ações necessárias sejam tomadas. É de responsabilidade do departamento atribuir um nível de prioridade.

É de responsabilidade de todos os integrantes da equipe de resposta a incidentes determinar a escala de disponibilidade para solução do incidente.

Uma vez corrigido, o Departamento de TI deve documentar o ocorrido, registrando todas as informações pertinentes para que possa ser criado um histórico de incidentes para uma possível recorrência.

3.2.3 Análise de Risco

As vulnerabilidades são possíveis fragilidades de um ativo ou grupo de ativos que podem ser exploradas por uma ou mais ameaças, resultando assim na quebra de um ou mais princípios da segurança da informação. Ao serem identificadas as vulnerabilidades ou pontos fracos, estes deverão ser classificados, identificando os riscos aos qual o ambiente está exposto e assim definindo medidas de segurança apropriadas para sua correção.

As ameaças podem ser consideradas como agentes externos ou internos ao ativo de informação, pois se aproveitam de sua vulnerabilidade para quebrar os princípios básicos da informação a confidencialidade, integridade ou disponibilidade.

Com relação à segurança, os riscos são compreendidos como condições que criam ou aumentam o potencial de danos e perdas, sendo medidos pela possibilidade de um evento vir a acontecer e produzir perdas.

Para evitar possíveis perdas de informação, o Departamento de TI tem a responsabilidade de gerir os riscos, onde os mesmos são identificados e classificados, determinando medidas de segurança para reduzi-los ou elimina-los.

RISCO = (Ameaça) x (Vulnerabilidade) x (Valor do Risco)

A classificação de risco deverá ser feita conforme estabelecido nesta política, respeitando os prazos para resolução e os fluxos de resposta e comunicação.

3.2.4 Avaliação e Classificação

A classificação dos incidentes ocorre por meio de dois indicadores principais: o impacto e a urgência. Cada um destes indicadores possui três níveis distintos: alto, médio e baixo.

A combinação entre a urgência para resolução do incidente, o impacto do incidente nos negócios e seu efeito provocado nos prazos e atividades define sua prioridade.

Código de Prioridade	Descrição	Prazo para solução
1	**Crítico**	**1 hora**
2	**Alto**	**8 horas**
3	**Médio**	**24 horas**
4	**Baixo**	**48 horas**
5	**Muito baixo**	**Planejado**

alto	**3**	**2**	**1**
médio	**4**	**3**	**2**
baixo	**5**	**4**	**3**
Impacto / Urgência	**baixo**	**médio**	**alto**

- **Crítico:** incidentes que comprometem gravemente a segurança dos ativos físicos e de informação da Total Biotecnologia / Biotrop, necessitando de tratamento imediato.
- **Alto:** incidentes que podem comprometer a segurança dos ativos físicos e de informação da Total Biotecnologia / Biotrop, porém com menor potencial de impacto adverso que os eventos críticos.
- **Médio:** incidentes que não possuem concomitantemente impacto e urgência altos.
- **Baixo e Muito Baixo:** incidentes que não afetam significativamente as operações da Total Biotecnologia / Biotrop

Os critérios supracitados possuem caráter subjetivo, sendo responsabilidade do Departamento de TI, determinar a categoria mais adequada em cada situação.

Os incidentes observados, bem como a solução adotada devem ser cadastrados em uma ferramenta de controle a fim de facilitar a sua solução em caso de recorrência. Este processo receberá o nome de base de conhecimento, aprimorando assim o tempo de resposta da equipe de TI.

3.2.5 Plano de Resposta a Incidentes

O Departamento de TI possui plena autonomia para decidir perante situações imprevistas ou inesperadas. Suas

ações em uma emergência devem contemplar as seguintes etapas:

- Definir equipe responsável por executar cada uma das atividades previstas no Plano;
- Procedimentos a serem seguidos imediatamente após a ocorrência de um incidente que possui potencial de impactar a Total Biotecnologia / Biotrop de maneira adversa;
- Definir a instalação reserva, com especificação dos bens de informática nela disponíveis, na qual os sistemas passarão a funcionar;
- Estabelecer a escala de prioridade dos aplicativos, de acordo com seu grau de interferência nos resultados operacionais e financeiros da Total Biotecnologia / Biotrop. Quanto maior a influência do aplicativo na capacidade de funcionamento da instituição, na sua situação econômica e na sua imagem, mais crítico ele será;
- Priorizar os arquivos, programas, para que os aplicativos críticos entrem em operação no menor tempo possível, mesmo que parcialmente;
- Identificar empresas responsáveis por oferecer serviços, equipamentos, suprimentos ou quaisquer outros bens necessários para a restauração;
- Procedimento necessário para restaurar os serviços computacionais na instalação reserva;
- Notificar o Comitê de Segurança da Informação sobre o ocorrido e as ações adotadas;
- Monitorar a situação até o retorno à normalidade das operações.
- Definir condições para ativação do Plano de Continuidade de Negócios.

3.2.6 Estratégias de Comunicação

O monitoramento das redes, servidores e sistemas é realizado continuamente pela equipe do Departamento de TI. Caso seja identificada uma anomalia por um membro da equipe, o mesmo deve informar o seu gestor explicando sobre o ocorrido. Após esta etapa, cabe a ele determinar quais deverão ser as ações a serem tomadas pela equipe de pronto atendimento.

Devido ao caráter emergencial deste processo, todas ações mitigadoras e/ou corretivas devem ser tomadas até que o problema seja resolvido. O Comitê de Segurança da Informação, conforme estabelecido na Política de Segurança da Informação, deve ser notificado por meio de e-mail ou reunião para debater o ocorrido.

Deve-se, então, elaborar um documento formalizando o ocorrido e as ações que foram tomadas para sua resolução, para prevenir que o incidente ocorra novamente.

3.2.7 Controle Contra Códigos Maliciosos

Visando à proteção contra ataques cibernéticos, a empresa deverá utilizar ferramentas e procedimentos para prevenir, detectar e/ou mitigar os riscos gerados por esses ataques, que podem causar prejuízos, gerar instabilidade e até mesmo a indisponibilidade do ambiente computacional.

Não é autorizada a instalação de qualquer software por usuários de dados computacionais. Somente o Departamento de TI realiza ou autoriza a instalação e atualização.

3.2.8 Sistemas de Firewall

Toda e qualquer atividade maliciosa dentro do ambiente de rede pode ser detectada pelo sistema de segurança da empresa. Se ainda assim houver, em um caso extremo de uma invasão ou brecha de segurança, o isolamento dos servidores atacados é feito imediatamente. Desse modo verifica-se o resultado do ataque e trata-se imediatamente os danos causados

3.2.9 Plano de Continuidade

O objetivo do Plano de Continuidade do Negócio é manter a integridade e a disponibilidade dos dados da Total Biotecnologia / Biotrop, bem como a disponibilidade dos serviços quando da ocorrência de situações fortuitas que comprometam o bom andamento dos negócios.

Possui ainda como objetivo, garantir que o funcionamento dos sistemas informatizados seja restabelecido no menor tempo possível a fim de reduzir os impactos causados por fatos imprevistos. O Plano deverá ainda, prever a possibilidade de dar continuidade nas operações produtivas em um ambiente de backup.

Visando garantir a correta execução do Plano de Continuidade o Departamento de TI deve definir e monitorar:

- Riscos a que está exposta a instituição, probabilidade de ocorrência e os impactos decorrentes (tanto aqueles relativos à escala do dano como ao tempo de recuperação);
- Consequências que poderão advir da interrupção de cada sistema computacional e operacional;
- Identificação e priorização de recursos, sistemas e processos críticos;
- Tempo limite para recuperação dos recursos, sistemas, processos;
- Alternativas para recuperação dos recursos, sistemas, processos, mensurando os custos e benefícios de cada alternativa.

12. PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: GESTÃO DE OPERAÇÕES

1. Objetivo

Este documento tem como objetivo descrever os processos operacionais dentro fluxo de trabalho relacionado à segurança da informação dentro de ambientes onde estão sendo tratados dados confidenciais na empresa.

2. Definições e abreviaturas

TI – Tecnologia da Informação

3. Descrição

3.1 Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que utilizam, mantêm ou lidam com dados confidenciais na Total Biotecnologia / Biotrop.

3.2 Seções da política e responsabilidades

3.2.1 Fluxo de Processo com Dados Confidenciais

Todos os materiais que possuem dados confidenciais, segundo a classificação, devem seguir o procedimento descrito a seguir, a fim de garantir a segurança da informação.

3.2.2 Procedimentos para Formatação de Computadores, Servidores e Mídias de Armazenamento

Quando houver a necessidade de se realizar a formatação de um computador, servidor ou mídia de armazenamento as seguintes etapas devem ser seguidas.

a. Preparação

- Backup dos arquivos pessoais dos usuários da máquina, quando necessário;
- Backup dos drivers;
- Backup de configurações de aplicativos;
- Listar aplicativos que estão instalados na máquina;

b. Processo de Formatação

- Verificar o particionamento do HD;
- Se necessário criar as partições de maneira correta;
- Instalar, configurar e atualizar o sistema operacional;
- Instalar os drivers;
- Instalar e configurar os programas necessários;

c. Pós-Formatação

- Restaurar o backup dos arquivos dos usuários;

- Testar todos os programas instalados;
- Testar conexões de rede e internet;
- Verificar ativação/registro do sistema operacional se necessário;

3.2.3 Procedimentos de Backup

É de responsabilidade do Departamento de TI, quando necessário, prever a realização de testes periódicos de restauração, no intuito de averiguar os processos de backup e estabelecer melhorias.

A administração dos backups também deve ser orientada para que seus trabalhos respeitem as janelas para execução, inclusive realizando previsão para a ampliação da capacidade dos dispositivos envolvidos no armazenamento.

As solicitações de restauração de arquivos deverão ser abertas formalmente através de ferramentas de abertura de chamados ou por e-mail. A solicitação deverá conter os nomes dos arquivos e pastas que deverão ser recuperados, o motivo da restauração e a data do arquivo que se pretende ter acesso.

3.2.4 Procedimento de Controle de Configurações/Alarmes

É de responsabilidade do Departamento de TI revisar as configurações gerais e de alarme da ferramenta de monitoramento, caso esta esteja implementada, objetivando a redução da vulnerabilidade dos sistemas internos da Total Biotecnologia / Biotrop a novas ameaças.

Para realização desta atividade devem ser seguidas as seguintes etapas de execução:

- Identificar o parâmetro a ser alterado/monitorado;
- Documentar na ferramenta de registro o detalhamento da alteração a ser realizada contendo as seguintes informações: ferramenta, alteração, motivo e vulnerabilidade identificada;
- Realizar a alteração;
- Monitorar o resultado desta configuração/alarme.

Este processo deve ser realizado pelo responsável quando forem identificadas possíveis vulnerabilidades dos sistemas internos.

3.2.5 Treinamento de Colaboradores

Quando houver mudanças nas políticas ou procedimentos, treinamentos específicos devem ser realizados para capacitar e informar os colaboradores relacionados. É de responsabilidade do Departamento de Treinamentos, ou quando não houver, de departamento especifico, desenvolverem metodologias e práticas para aplicação e registro destes treinamentos. Os treinamentos devem ser documentados por meio de controles de presença. É recomendada a aplicação de avaliação do treinamento baseados nos seguintes critérios:

- Metodologia utilizada
- Conteúdo
- Aplicabilidade
- Avaliação de Satisfação.

13. PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: GESTÃO DE SISTEMAS DE INFORMAÇÃO E INFRAESTRUTURA

1. Objetivo

Este documento tem como objetivo definir os processos de gerenciamento dos sistemas de informação e infraestrutura da empresa.

2. Definições e abreviaturas

TI – Tecnologia da Informação

3. Descrição

3.1 Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que utilizam os sistemas de informação e a infraestrutura da empresa.

3.2 Seções da política e responsabilidades

3.2.1 Correções (*Patch Management*)

Para minimizar as ameaças de vulnerabilidade, a Total Biotecnologia / Biotrop deve ter sistemas configurados adequadamente, utilizar os softwares mais recentes e instalar as atualizações de software recomendadas. Cabe ao gestor avaliar e manter a integridade de softwares em um ambiente de rede, por meio de um procedimento de atualização de correções.

O gerenciamento é considerado crítico para servidores de aplicativos que controlam a infraestrutura central ou de negócios, como servidores de arquivos, impressão, servidores que controlam o serviço de diretório e assim por diante.

É responsabilidade do Departamento de TI garantir que os servidores devem usar versões de softwares com atualizações mais recentes. O procedimento para atualização das correções deve ser realizado conforme as etapas descritas a seguir:

a. Fase 1: Avaliar o Ambiente (continuamente)

O Departamento de TI monitora os servidores regularmente por meio de software se implementado para identificar qualquer vulnerabilidade no ambiente que possa ser considerada crítica. Se um servidor for considerado em situação não segura, ele será atualizado por prioridade.

b. Fase 2: Identificar Novas Atualizações

O processo de implantação de uma atualização em todos os servidores começa após a divulgação de boletins de atualização, que são identificados pelos colaboradores responsáveis.

As atualizações são classificadas de acordo com os seguintes critérios de gravidade:

- **Crítica.** Uma vulnerabilidade cuja exploração pode permitir a propagação de um vírus (worm) da Internet sem a ação do usuário. Devem ser executadas em até uma semana.
- **Importante.** Uma vulnerabilidade cuja exploração pode causar o comprometimento da confidencialidade, da integridade ou da disponibilidade dos dados do usuário, ou o comprometimento da integridade ou da disponibilidade de recursos de processamento. Devem ser executadas em até 30 dias.
- **Moderada.** Uma atualização corretiva sem impacto de vulnerabilidade. Para esta categoria não se define um prazo máximo de execução.

c. Fase 3: Avaliar e Planejar a Implantação da Atualização

O Departamento de TI deve avaliar todos os impactos que a atualização ocasionará na rede interna de computadores e em sua utilização pelos usuários. Visando reduzir tais impactos adversos, os colaboradores responsáveis programam as atualizações para serem realizadas durante a madrugada ou fora do horário de atividade da empresa.

3.2.2 Controle de Redes

Os controles de redes deverão ser realizados através de regras de bloqueios no firewall quando existente, com configuração de perfil do usuário no computador, configuração de extensão de arquivos em e-mails e rotinas de verificação de portas abertas e reputação na internet. Devem ser usadas as ferramentas abaixo, habilitadas para garantir o controle e segurança da rede:

IPS (Intrusion Prevention System): realiza a inspeção dos pacotes usando assinaturas de ataques conhecidos para identificar códigos maliciosos e bloqueá-los.

Controle de aplicações (Application Control): permite a granularidade do controle de acesso a aplicações como: Skype, TeamViewer, Messenger, Logmein, Facebook, Twitter, Instagram etc. O controle de aplicações funciona também para bloquear aplicações indesejadas que atravessam sistemas de segurança quando sua conexão seja criptografada ou usa a mesma porta de um outro serviço. As assinaturas são atualizadas automaticamente pelo fabricante.

Controle de reputação (Reputation): bloqueia ou libera automaticamente páginas com reputação ruim, para HTTP e para HTTPS (para HTTPS depende do DPI habilitado—Deep Inspection) conforme sua configuração. Limitar um acesso a um site que possui uma má reputação é extremamente importante, pois se o mesmo está com uma reputação ruim, provavelmente está vulnerável a ataques.

Aplicação do Safe Search: controla a pesquisa de conteúdo impróprio nos principais mecanismos de busca da internet, impedindo que um usuário consiga encontrar sites com pornografia, crimes cibernéticos, entre outros. O filtro é baseado no próprio projeto safesearch. Por exemplo: o usuário busca as palavras "PORNOGRAFIA" ou "PEDOFILIA" no site do Google, mas será impedido de localizar conteúdos impróprios após habilitação do Safe Search.

Os e-mails não podem trafegar com arquivos com extensões consideradas perigosas. Caso o usuário necessite receber ou enviar um arquivo com extensão bloqueada, o seu gestor deve solicitar através de um e-mail ao Departamento de TI a liberação do mesmo temporariamente.

Os perfis dos usuários nos computadores devem ser cadastrados como “Usuário Padrão” ou “Convidado” tendo acesso diferenciado do usuário “Administrador local”. Somente o Departamento de TI possuirá a senha do usuário “Administrador local” dos computadores.

3.2.3 Instalação e Proteção dos Equipamentos

A sala onde estão instalados os ativos de TI como por exemplo servidores, equipamentos de telefonia e internet,

deve ser refrigerada e monitorada por câmeras quando possível. A recomendação é de que o acesso à sala de servidores, equipamentos de telefonia e internet só poderá ser feito pelo departamento de TI ou com o acompanhamento e/ou autorização deste. Para a proteção de equipamentos deverá haver rede elétrica estabilizada, geradores e nobreak quando possível com a duração da bateria de aproximadamente 1 hora e meia.

15. PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: SEGURANÇA FÍSICA E DO AMBIENTE

1. Objetivo

Este documento tem como objetivo descrever os dispositivos de segurança das instalações físicas da empresa.

2. Definições e abreviaturas

TI – Tecnologia da Informação.

3. Descrição

3.1 Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que tem ou necessitam de acesso às dependências comuns ou restritas da Total Biotecnologia / Biotrop.

3.2 Seções da política e responsabilidades

3.2.1 Controle de Entrada Física

O controle de entrada física para colaboradores e visitantes deve ser realizado por meio de monitoramento de câmeras, equipamentos de controle de acesso e portões de entrada com sistema de “torniquetes” e catracas quando possível.

A solicitação para liberação de acesso de visitantes só pode ser realizada pela diretoria, gerência ou responsáveis pelos departamentos.

Quando existente, a Recepção é responsável por realizar o cadastramento de visitantes, clientes, fornecedores e prestadores de serviço. Sempre um funcionário deverá acompanhar o visitante, cliente ou fornecedor, sendo responsável pela circulação dos mesmos nas dependências da Total Biotecnologia / Biotrop. Para os prestadores de serviço é solicitada a presença de um técnico de segurança do trabalho quando existente ou funcionário direcionado durante a execução do trabalho ou prestação do serviço.

A entrada de visitantes, clientes, fornecedores e prestadores de serviço podem ser previamente autorizadas quando solicitada por e-mail. Todos os visitantes, clientes, fornecedores e prestadores de serviços devem ser identificados.

3.2.2 Segurança em escritórios, salas e instalações

A segurança dos departamentos, salas e instalações com acesso restrito da Total Biotecnologia / Biotrop será realizada através de um sistema de controle de acesso com equipamentos de liberação de portas e sistema de monitoramento por câmeras. Somente o responsável pelo departamento pode autorizar ou restringir o acesso. A solicitação deve ser formalizada via e-mail e encaminhada para o departamento em questão para realizar o cadastro e liberação.

16. PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: MESA E TELA LIMPA

1. Objetivo

Este documento tem como objetivo descrever os procedimentos de utilização dos recursos da empresa, bem como dispor de seus objetos pessoais e tratamento de objetos e documentos sobre as mesas, assim como a disposição da área de trabalho de seus computadores nas instalações físicas da empresa.

2. Definições e abreviaturas

TI – Tecnologia da Informação.

3. Descrição

3.1 Aplicação

Esta política se aplica a todos os colaboradores, e parceiros que se utilizam das salas, mesas e escritórios da Total Biotecnologia / Biotrop.

3.1.1 Responsabilidades

Uma Política de Mesa Limpa e Tela Limpa se refere a práticas relacionadas a assegurar que informações sensíveis, tanto em formato digital quanto físico, e ativos não fiquem desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso, ou quando alguém deixa sua área de trabalho, seja por um curto período de tempo ou ao final do dia.

Uma vez que informações e ativos em uma área de trabalho estão em um de seus lugares mais vulneráveis, sujeitos a divulgação ou uso não autorizado, a adoção da Política de Mesa Limpa e Tela Limpa é uma das principais estratégias a se utilizar na tentativa de reduzir os riscos de brechas de segurança. E, felizmente, muitas das práticas requerem baixa tecnologia e fáceis de implementar, as quais deverão ser implementadas:

- Uso de áreas com trancas: gavetas com trancas, armários de pastas, cofres e salas de arquivo devem estar disponíveis para armazenar mídias de informação ou dispositivos facilmente transportáveis quando não em uso, ou quando não houver ninguém tomando conta deles. Além da proteção contra acesso não autorizado, esta medida também pode proteger a informação e ativos contra desastres tais como incêndios, terremotos, inundações ou explosões;
- Proteção de dispositivos e sistemas de informação: computadores e dispositivos similares devem estar posicionados de tal forma a evitar que transeuntes tenham a chance de olhar as telas, e configurados para usar protetores de tela ativados por tempo e protegidos por senha, para minimizar as chances de que alguém tire vantagem de equipamentos desacompanhados.
- Adicionalmente, sistemas de informação deveriam ter sessões encerradas quando não em uso. Ao final do dia os dispositivos deveriam ser desligados, especialmente aqueles conectados em rede;
- Restrições ao uso de tecnologias de cópia e impressão: o uso de impressoras, scanners e câmeras, por exemplo, deve ser controlado, pela redução de sua quantidade ou pelo uso de funções de código que permitam que somente pessoas autorizadas tenham acesso ao material enviado a elas. E, qualquer informação enviada a impressoras deveria ser recolhida tão rapidamente quanto possível;
- Adoção de uma cultura sem papel: documentos não devem ser impressos desnecessariamente, e lembretes não devem ser deixados em monitores ou sob teclados. Lembre-se, mesmo pequenos

pedaços de informação podem ser o suficiente para pessoa mal-intencionadas descobrirem aspectos de sua vida, ou dos processos da empresa, que possam ajudá-los a comprometer informações;

- Descarte de informações deixadas em salas de Reunião e Diretoria: todas as informações em quadros brancos devem ser apagadas e todos os pedaços de papel usados durante a reunião devem estar sujeitos a um descarte apropriado.

3.1.2 Controle

Assegurar que as informações do negócio sensíveis ou críticas, por exemplo, em papel ou em mídia de armazenamento eletrônicas, sejam guardadas em lugar seguro (idealmente em um cofre, armário ou outras formas de mobília de segurança) quando não em uso, especialmente quando o escritório está desocupado;

Assegurar que os computadores e terminais sejam mantidos desligados ou protegidos com mecanismo de travamento de tela e teclados controlados por senha, token ou mecanismo de autenticação similar quando sem monitoração e protegida por tecla de bloqueio, senhas ou outros controles, quando não usados;

Garantir que sejam evitados o uso não autorizado de fotocopiadoras e outra tecnologia de reprodução (por exemplo, scanners, máquinas fotográficas digitais);

Garantir que os documentos que contêm informação sensível ou classificada sejam removidos de impressoras imediatamente.

3.1.3 Informações Adicionais

A ISO 27001, um framework popular de segurança da informação, e a ISO 27002, um código de prática detalhado, dá orientação, por meio do controle de segurança – Política de Mesa Limpa e Tela Limpa. Vejamos com mais detalhes:

Adotar política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.

Assegurar que a Política de Mesa Limpa e Tela Limpa protegida leve em consideração a classificação da informação, requisitos contratuais e legais, e o risco correspondente e aspectos culturais da empresa. Convém que as seguintes regras sejam consideradas:

Uma Política de Mesa Limpa e Tela Limpa protegida reduz o risco de acesso não autorizado, perda e dano da informação durante e fora do horário normal de trabalho. Cofres e outras formas de recursos de armazenamento seguro também podem proteger informações armazenadas contra desastres como incêndio, terremotos, enchentes ou explosão.

17. PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: DISPOSITIVOS MÓVEIS

1.Tratativa

Anexo PSI 05_Política de Dispositivos Móveis - Total Biotecnologia Biotrop.

18. PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: TRABALHO REMOTO

1.Tratativa

Anexo PSI 04_Política de Trabalho Remoto - Total Biotecnologia Biotrop.

19. PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: SANÇÕES POR DESCUMPRIMENTO DA PSI

1. Objetivo

Este documento tem como objetivo descrever as sanções previstas em nosso regulamento interno para o descumprimento ou falta de atenção as políticas internas.

2. Definições e abreviaturas

TI – Tecnologia da Informação.

3. Descrição

3.1 Aplicação

Esta política se aplica a todos os colaboradores que conhecem as normas e regulamentos internos, bem como as políticas de segurança internas.

3.2 Seções da política e responsabilidades

3.2.1 Caracterização

As informações confidenciais necessárias ao seu trabalho devem ser usadas apenas com essa finalidade. Essas informações devem ser compartilhadas apenas com outros colaboradores que precisem delas para seu trabalho e que tenham autorização de acesso às mesmas.

3.2.2 Sanções

As sanções deverão ser definidas pelo departamento responsável. O descumprimento subsequente de toda e qualquer norma e regulamento da empresa deve ser levado em conta no momento da elaboração das mesmas.