PO.19 Segurança da Informação

Diretoria: TI
Gerência: Governança de TI e Arquitetura

Criação: 14/04/2011
Última revisão: 27/03/2024

1. OBJETIVO

Esta Política estabelece diretrizes e padrões de Segurança da Informação para a Dexco, visando proteger a confidencialidade, integridade e disponibilidade dos ativos de informação.

2. ABRANGÊNCIA

Esta Política se aplica a todas as áreas da Companhia, seus administradores e colaboradores, bem como a terceiros que eventualmente venham a ser contratados pela Dexco S.A. e que a representem nas atividades aqui referidas.

3. REFERÊNCIAS NORMATIVAS

- NO.44 Aplicação de Medidas Disciplinares;
- NO.56 Gestão de Acessos de TI;
- NO.57 Utilização de Recursos de Microinformática;
- NO.58 Classificação da Informação;
- NO.59 Gestão de Vulnerabilidade;
- NO.63 Gestão de Backup e Restore.

4. DEFINIÇÕES

Confidencialidade: Refere-se a assegurar que todos os meios de processamento e/ou conservação de informação contenham medidas de proteção quanto ao acesso e utilização por pessoa não-autorizada, assegurando que toda informação esteja protegida de revelações acidentais, espionagem industrial, violação da privacidade e outras ações similares.

Integridade: Refere-se a assegurar que todas as informações processadas, transacionadas ou armazenadas nas bases e sistemas da Dexco estejam livres de alterações indevidas e irregularidades de qualquer espécie.

Disponibilidade: É a garantia que a informação e sua capacidade de processamento, manual ou automática, sejam resguardadas e recuperadas sempre que necessário, de modo a não impactar significativamente o andamento dos negócios, estando sempre ao dispor da entidade que a solicitar.

Incidente de Segurança da Informação: Qualquer ação que infrinja um ou mais pilares de Segurança de Informação (integridade, confidencialidade e disponibilidade)

Ativo: Qualquer item que tenha valor para a Dexco, tais como, mas não se limitando a: informações, estrutura física, ambientes tecnológicos.

Backup: Cópia de segurança dos dados (informações) ou sistema (aplicativos, softwares) de um dispositivo de armazenamento para outro ambiente, a fim de que esses mesmos dados possam ser restaurados em caso de incidente de Segurança da Informação.

Colaboradores: todos os profissionais contratados que possuem vínculo empregatício com a Dexco, incluindo os estagiários e menores aprendizes.

Terceiros: Prestadores de serviço ou empresas contratadas para fornecimento de serviço e/ou mão de obra para a Dexco.

Software ITSM: Aplicação utilizada para abertura e gerenciamento de chamados, bem como gestão de projetos.

Plano de Gestão de Incidentes: Documento que descreve como o incidente de Segurança da Informação deve ser gerenciado, contando com uma árvore de contato das pessoas chaves dos processos críticos da companhia.

NDA (Non-Disclosure Agreement): O termo de confidencialidade visa proteger e resguardar dados da Companhia, como novos desenvolvimentos, processos, projetos, produtos, informações de custos e preços, negociações, fornecedores e clientes contra divulgação não autorizada.

5. PAPÉIS & RESPONSABILIDADES

5.1 Segurança da Informação

- Aprovar e revisar periodicamente esta e demais políticas e normas relacionadas à Segurança da Informação;
- Garantir os recursos necessários para a implantação de controles de segurança;
- Definir regras para gerenciamento do ambiente tecnológico, com as melhores práticas de Segurança da Informação;
- Garantir o cumprimento das legislações e regulamentações vigentes, no que tange a Segurança da Informação da Dexco;
- Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e implantar medidas corretivas para reduzir os riscos;
- Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado;
- Gerenciar as revisões de acessos periódicas dos sistemas escopo de auditoria;
- Administrar o programa de conscientização de cibersegurança.

5.2 Infraestrutura

- Seguir todas as diretrizes desta Política;
- Cumprir as definições de gerenciamento do ambiente tecnológico proposto pela área de Segurança da Informação.

5.3 Service Desk

- Encaminhar tempestivamente para a área de Segurança da Informação os chamados de incidentes de Segurança da Informação abertos no software ITSM.

5.4 Colaboradores

- Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;
- Assinar o Termo de Compromisso "PO-19 - Termo de Compromisso;" formalizando a ciência e o aceite integral das disposições da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento e respeitando a confidencialidade, a integridade e a disponibilidade das informações da Dexco;
- Proteger as informações contra acesso, divulgação, modificação ou destruição não autorizados pela Dexco;
- Realizar o descarte adequado de documentos de acordo com seu grau de classificação;
- Utilizar os equipamentos e recursos tecnológicos e exclusivamente para os fins a que foram destinados e de interesse da Dexco;
- Respeitar o caráter confidencial das senhas de acesso aos ativos de TI que lhe forem concedidas;
- Comunicar a área de Segurança da Informação, qualquer evento que viole esta Política ou que possa vir a colocar em risco a segurança das informações da Dexco;
- Em caso de dúvidas e/ou pedidos de esclarecimento sobre esta Política, contatar o time de Segurança da Informação: segurancadigital@dex.co

5.5 Gestores

- Cumprir e fazer cumprir esta Política em sua equipe;
- Exigir dos terceiros a assinatura do termo de confidencialidade referente às informações às quais terão acesso, conforme classificação da informação;
- Aprovar as requisições de acessos considerando a função exercida pelo requisitante, segregação de função e princípio de menor privilégio;
- Revisar periodicamente os acessos de sua equipe de maneira tempestiva, sempre que necessário ou solicitado por Segurança da Informação
- Solicitar o cancelamento imediato do acesso aos ativos de TI de todo terceiro sob a sua gestão, que seja desligado ou transferido de função;
- Aplicar as penalidades contidas na norma "NO.44 Aplicação de Medidas Disciplinares" em caso do não cumprimento desta Política pelo seu liderado;
- Orientar a devida classificação da informação de seus colaboradores.

5.6 Recursos Humanos

- Atribuir aos colaboradores na fase de formalização do contrato individual de trabalho, estágio, entre outros, a incumbência do cumprimento das responsabilidades para a manutenção da segurança da informação, através da assinatura do termo "PO-19 - Termo de Compromisso";
- Reportar imediatamente qualquer desligamento para que todos as medidas cabíveis sejam tomadas, conforme disposto na norma "NO.56 Gestão de Acesso de TI".

5.7 Compliance

- Disponibilizar e divulgar esta Política aos colaboradores da Companhia, além de outras Normas relacionadas à Segurança da Informação.

6. PROCEDIMENTOS

6.1 Classificação da Informação

As informações da Dexco podem estar presentes em sistemas e em diversos tipos de mídia como: papel, mídias removíveis (CD, DVD, pendrive, HD, dentre outros), bem como na comunicação verbal e devem ser protegidas de acordo com sua classificação e relevância para o negócio.

Desta forma, toda informação de uso corporativo deve ser classificada pelo proprietário da informação, considerando-se os quatro níveis descritos a seguir:

- Confidencial: As informações são disponibilizadas somente para indivíduos autorizados previamente e o acesso não autorizado às informações pode causar danos significativos aos negócios e/ou à reputação da organização. Geralmente para esses casos se faz necessário assinatura do termo de *NDA* (*Non-Disclosure Agreemen*t).
- Restrito: As informações são disponibilizadas somente a um grupo específico de colaboradores e terceiros autorizados, e se divulgadas indevidamente podem causar danos consideráveis ao negócio.
- Uso Interno: As informações são disponibilizadas a todos os colaboradores e à alguns terceiros com regras de controle de acesso, e sua utilização deve ser limitada para utilização internamente na Dexco.
- Público: As informações estão ou podem estar disponíveis para o público em geral, inclusive externamente, e geralmente trata-se de informações de baixa sensibilidade.

As informações possuem ciclo de vida e devem ser reclassificadas regularmente de acordo com as mudanças em seu valor, sensibilidade e criticidade pelo Proprietário da Informação. Demais informações e diretrizes deverão ser consultados na norma “NO.58 Classificação da Informação”.

6.2 Gestão de Acessos

Os acessos só poderão ser concedidos após a assinatura do contrato de trabalho/prestação de serviço ou assinatura do NDA, para garantir o sigilo e bom uso das informações conforme expresso neste documento e normas aplicáveis.

Deve-se criar logins únicos e identificáveis para os usuários, sendo da responsabilidade dos colaboradores a utilização de seus logins para fins devidos ao seu escopo de trabalho, bem como e salvaguarda segura de suas senhas, incluindo a utilização do e-mail corporativo que não deverá ser compartilhado externamente, para uso pessoal, sendo todos os logins de uso único, intransferível, sendo vetado qualquer compartilhamento.

Os acessos dos usuários terceiros são de responsabilidade compartilhada entre a parte terceira e o gestor contratante, portanto, assim que a prestação de serviço cessar é de responsabilidade do gestor solicitar o desligamento do acesso imediatamente.

A concessão de acessos deve seguir com o critério de menor privilégio, a partir da premissa de permissões necessárias e suficientes para que um colaborador possa realizar suas atividades, por um tempo limitado e com os direitos mínimos necessários para as suas tarefas, seguindo as diretrizes da Norma “NO.56 Gestão de Acessos de TI”.

Os gestores são responsáveis por avaliar, revisar e aprovar os acessos solicitados pelos seus subordinados e em caso de desvio de conduta mediante aprovações indevidas, poderão ser responsabilizados.

Nos casos em que não houver revisão dos acessos por parte dos gestores ou mediante indício de uso indevido pelo usuário, a equipe de Segurança da Informação revogará os acessos.

A utilização de recursos de rede, sistemas, equipamentos e outras fontes de informação são monitorados e podem ser coletadas e utilizadas, a critério da Dexco, para a execução de investigações internas ou para atendimento de medidas judiciais, sem aviso prévio às pessoas envolvidas, respeitando a privacidade dos colaboradores, sempre que necessário.

6.3 Gestão de Ativos

Os ativos de Tecnologia da Informação devem ser categorizados, inventariados e gerenciados durante todo o seu ciclo de vida, inclusive no descarte, que deve ser realizado de modo a preservar a confidencialidade das informações e minimizar possíveis impactos ambientais.

O acesso às mídias removíveis é bloqueado nas estações de trabalho da Dexco, restrita somente às pessoas que necessitem desse recurso para desenvolver suas atividades, unicamente para exercício da função contratada, sendo estritamente vetada a utilização para fins pessoais.

Os ativos da Dexco devem ser tratados de forma sigilosa e ética, de acordo com as leis vigentes e normativos internos, promovendo o uso adequado e prevenindo a exposição indevida das informações.

6.4 Criptografia

Todos os notebooks Dexco contam com criptografia aplicada, a fim de garantir a confidencialidade e autenticidade das informações, conforme norma “NO.57 Utilização de Recursos de Microinformática”.

6.5 Gestão de Incidentes de Segurança da Informação

Qualquer evento adverso, relacionado à segurança de um ativo que pode prejudicar quaisquer princípios da Segurança da Informação (confidencialidade, integridade e disponibilidade) deverá ser reportado ao time de Segurança da Informação, onde de maneira tempestiva será tratado e gerenciado conforme o Plano de Gestão de Incidentes.

6.6 Gestão de Vulnerabilidade

A área de Segurança da Informação deve realizar avaliações de vulnerabilidades periodicamente para identificar e remediar possíveis fragilidades de segurança no ambiente tecnológico da Dexco.

A gestão de vulnerabilidade deve ser conduzida de acordo com o disposto na norma: “NO.59 Gestão de Vulnerabilidade”.

6.7 Backup

As informações consideradas críticas utilizadas nas atividades da Dexco devem ter cópias de segurança.

As cópias de segurança devem atender aos requisitos operacionais, legais, históricos e de auditoria, como quanto à sua periodicidade de geração e salvaguarda.

A cópia de segurança e sua restauração deverão seguir o procedimento descrito na norma “NO.63 Gestão de Backup e Restore.”

6.8 Segurança Física

A entrada aos Data Centers tem acesso devidamente controlado e monitorado.

As áreas do Data Center devem ser protegidas com barreiras de segurança ou mecanismos de acesso, de forma a impedir o acesso não autorizado.

O acesso ao Datacenter sem as devidas identificações só poderá ocorrer em emergências, quando a segurança física do Datacenter for comprometida, como por incêndio, catástrofes naturais ou abalo da estrutura predial.

6.9 Mesa e Tela Limpa

Para reduzir o risco de violação de segurança, fraudes e vazamento de informações causadas por documentos, deixados sobre a mesa ou à mostra na tela dos equipamentos das instalações da empresa, faz-se necessário que documentos em meios físicos e/ou eletrônicos não permaneçam sobre a mesa ou aplicação desnecessariamente, devendo ser devidamente manipulados, armazenados e descartados. Adicionalmente, todos os usuários devem bloquear o equipamento ao se ausentar do mesmo.

6.10 Conscientização em Cibersegurança

A Dexco promove periodicamente campanhas de conscientização de forma presencial e/ou online, abordando as melhores práticas em Segurança da Informação, com o objetivo de fortalecer a cultura de cibersegurança na companhia. Essas campanhas podem ser veiculadas através de e-mails informativos, intranet da empresa, *e-learning,* mídia *indoor*, e outros meios que a equipe de Segurança julgar necessário.

7. SANÇÕES

Descumprimentos às diretrizes desta Política estarão sujeitos à aplicação das medidas disciplinares cabíveis.

No caso de descumprimento das diretrizes presentes nesta Política, a área de Compliance deverá ser comunicada pela caixa departamental compliance@dex.co, oportunidade em que acionará as áreas pertinentes para apuração dos fatos e, se necessário, serão aplicadas medidas disciplinares.

Caso a própria Segurança da Informação identifique violações quanto às diretrizes contidas nesta norma, ocorrerá a comunicação desta área para o Gestor do Usuário, com a anuência do RH da unidade, sobre a violação realizada. Caberá ao Gestor do Usuário a aplicação das penalidades contidas na norma “NO.44 Aplicação de Medidas Disciplinares”.

8. VIGÊNCIA

Esta Política passará a vigorar a partir da sua data de publicação e deve ser revisada a cada 3 (três) anos, e poderá ser alterada em qualquer tempo, sempre que necessário.

9. APROVAÇÃO

Esta Política foi aprovada pelo Conselho de Administração da Dexco.

10. ANEXOS

- PO-19 - Termo de Compromisso;
- Plano de Gestão de Incidentes de Segurança Cibernética.


DEXCO
Deca Portinari Hydra Duratex Castelatto Ceusa Durafloor