Sumário

1. OBJETIVO

.
Estabelecer e definir a implementação de práticas de Segurança, e registrar os controles de segurança de IT (Information Technology) que serão implementados para do **Grupo CPFL**.

Este documento estabelecerá um relacionamento de controles de segurança entre a DXC e o do **Grupo CPFL**, baseado na seção do contrato onde estão definidas as responsabilidades relacionadas à segurança.
A DXC oferecerá controles de segurança consistentes com os controles de segurança existentes, e irá trabalhar para desenvolver um documento detalhado que definirá os controles estabelecidos em um acordo mútuo que a DXC irá implementar.

2. ÂMBITO DE APLICAÇÃO

2.1. Empresa
Todas as empresas do **Grupo CPFL**.

2.2. Área
Todos os colaboradores envolvidos na prestação de serviços, que tenham interface com o processo de Segurança da Informação.

3. DEFINIÇÕES

Grupo CPFL: A CPFL Energia S.A., e todas as suas controladas diretas e/ou indiretas, exceto as empresas com seus próprios padrões de governança e gestão que compartilham controle com outras empresas.

A – Auxilia
E - Executa
InsightVM – Ferramenta de Compliance e Vulnerabilidades para análise do ambiente

4. DOCUMENTOS DE REFERÊNCIA

Baseado nas melhores práticas de Segurança de Mercado para os Itens acordados no Contrato.

5. RESPONSABILIDADES

5.1. DXC

É responsável por garantir a aplicação dos controles de segurança no ambiente e garantir que esteja aplicado, monitorado e qualquer desvio apresentado ao do **Grupo CPFL**.

5.2. Grupo CPFL

Deve definir os parâmetros que serão customizados ao ambiente, e caso haja alguma alteração ou problema notificar a DXC.

Funções Gerais			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	**Grupo CPFL**	**N/A**
Efetuar a Gestão diária dos Processos de Segurança	**E**	**E**	**-**
Revisar adendos às políticas e padrões de segurança do **Grupo CPFL**. Notificar a DXC se tais mudanças podem ou não ser implementadas e que, caso sejam implementadas, serão consideradas como um Novo Serviço.	**A**	**E**	**-**
Comunicar os procedimentos de segurança aos usuários do **Grupo CPFL** afetados por este serviço, tais como procedimentos de login, utilização de senhas, utilização de programas antivírus e segurança para dados e equipamentos.	**A**	**E**	**-**

6. REGRAS BÁSICAS

6.1. Criação/Manutenção

Os valores 'Requeridos' pelo **Grupo CPFL** serão as políticas de segurança utilizadas na implementação dos serviços de segurança.

Criação/Manutenção do documento			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Durante o período de transição, desenvolver o documento detalhado "Políticas de Segurança da Informação" (este documento)	**E**	**E**	**-**
Manter o controle do documento "Política de Segurança Operacional do Data Center" (este documento)	**E**	**E**	**-**
Rever as políticas e procedimentos de segurança para que sejam efetivos e recomendar melhorias.	**E**	**E**	**-**
Notificar a DXC em relação às mudanças nas políticas e nos padrões de segurança definidos, antes da implementação.	**A**	**E**	**-**

6.2. Manual de Implementação (insightVM)

A ferramenta contém especificações técnicas para sistemas operacionais e outros softwares de sistemas com registros de controles específicos necessários para implementar a política de Segurança definida neste documento.
Toda a parametrização é feita através da ferramenta.

6.3. Controles Físicos de Segurança

Controles Físicos de Áreas sob controle da DXC

Furtos ou danos aos recursos de processamento de informações, divulgação ou remoção de informações e interrupção de suporte para processos de negócios são riscos que os gerentes que são proprietários ou são responsáveis pelo processamento de informações devem avaliar. Como o acesso físico aos recursos de processamento de informações os expõe a todos estes riscos, o gerenciamento deve instituir os controles de acesso físico que sejam proporcionais ao risco e possível perda.

Esta seção abordará os controles para proteger os centros de dados sob controle da DXC.

Controles Físicos de Áreas sob controle da DXC no Grupo CPFL

Onde a DXC tiver responsabilidade e controle de uma área de centro de processamento de dados em uma localização do **Grupo CPFL**, os padrões e critérios documentados no restante deste capítulo serão implementados. Se alguns dos controles físicos não puderem ser implementados, eles serão documentados no final desta seção.

Controles Físicos de Áreas que não estão sob controle da DXC no Grupo CPFL

Onde a DXC tiver responsabilidade pelo hardware de centro de processamento de dados em uma localização do **Grupo CPFL** no qual o **Grupo CPFL** tem responsabilidade pelo gerenciamento e controle, o seguinte procedimento é recomendado como um controle mínimo:

- A área deve ter um proprietário do **Grupo CPFL** denominado
- A área deve ser trancada mesmo quando houver pessoas trabalhando
- O acesso à área deve ser restrito apenas a pessoas autorizadas pelo proprietário
- O acesso à área deve ser controlado pelo sistema eletrônico de controle de acesso utilizando alguma forma de dispositivo de leitura
- A lista de acesso deve ser verificada pelo proprietário mensalmente
- A documentação do sistema de gerenciamento e controles devem ser fornecidos à DXC pelo proprietário

Segurança Física			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Prover controles físicos de segurança nas instalações da DXC	**E**	**-**	**-**
Prover controles físicos de segurança nas instalações do **Grupo CPFL**	**A**	**E**	**-**

Acesso ao Centro de Processamento de Dados

O acesso aos centros de processamento de dados sob controle da DXC deve ser estritamente limitado a funcionários da DXC cujas responsabilidades de trabalho estão dentro do centro de processamento de dados e a outras pessoas que precisam de acesso por clara necessidade de negócios. O gerente do **Grupo CPFL** responsável pelo centro de processamento de dados, ou seu encarregado, deve aprovar todos os pedidos de acesso permanente ao centro de processamento de dados, incluindo fornecedores sob contrato.

Centro de Processamento de Dados (Data Center Campinas, RGE, DR)			
Funções/Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Restringir o acesso a todas as áreas de processamento de dados apenas a pessoas autorizadas, se nas instalações do **Grupo CPFL** ou da DXC, pelas quais a DXC tem responsabilidade de segurança	**E**	**A**	**-**

6.4. Áreas Controladas

Para alcançar um alto nível de segurança, níveis diferentes de controle devem ser implementados. Isso aumenta a eficácia da segurança física dos sistemas e dos ativos gerenciados pela DXC, impedindo acesso não autorizado, dano aos ativos ou interrupção de serviços. As áreas controladas são utilizadas para manter instalados plataformas de médio porte, ou sistemas distribuídos e mídia de armazenamento portátil. O nível requerido para os controles de acesso físico está baseado na determinação da importância do serviço que está sendo prestado e o valor dos equipamentos de processamento de

informações. Áreas de controle “Restritas” são as áreas mais seguras, seguidas das áreas de controle “Protegidas”.

Requisitos Físicos para Áreas Controladas

Esta seção estabelece os requisitos físicos para as áreas controladas dentro dos centros de dados.

Requisitos Físicos	Áreas Controladas	
	Protegido	Restrito
Acesso apenas a áreas de construção às quais o público geral não tem acesso.	Sim	Sim
Proprietário da área claramente identificado.	Sim	Sim
A área deve ser trancada, mesmo quando ocupada.	Sim	Sim
As saídas de emergência devem ter alarmes em funcionamento, audíveis e monitorados. Por razões de segurança, os alarmes devem funcionar alimentados pelo sistema de emergência e os eventos de alarme devem ser investigados. Deve ser executada e documentada uma verificação periódica para determinar se os alarmes de saída de emergência estão funcionando.	Não	Sim
Não são permitidas janelas externas em instalações de andares térreos construídas após 1º de julho de 1992, a menos que seja utilizado vidro resistente a impacto.	Não	Sim
A área deve incluir barreiras de laje-a-laje OU um sistema de detecção de invasores.	Não	Sim
O acesso à área deve ser controlado por um sistema eletrônico de controle de acesso, exceto quando liberado especificamente pelo Diretor do proprietário da área ou por um executivo de nível equivalente.	Não	Sim

Gerenciamentos de Áreas Controladas

Os proprietários da área são responsáveis por manter controles de negócios eficazes sobre a mesma. O controle pode ser feito por diversos meios. Chaves, travas codificadas, CAS (Controlled Access Systems) ou entradas vigiadas por guardas, são todos exemplos de controle de acesso físico.

Requisitos de Acesso	Áreas Controladas	
	Protegido	Restrito
O acesso é controlado para limitar a entrada na área apenas a pessoas autorizadas. As pessoas incluídas na lista de acesso aprovado estão autorizadas.	Sim	Sim
O acesso temporário para visitantes deverá ser concedido por uma pessoa autorizada.	Sim	Sim
As pessoas com acesso autorizado devem ter uma necessidade de acesso de negócios vigente e serem autorizadas pelo proprietário da área. Supõe-se que o proprietário da área determinará o que é uma necessidade de acesso de negócios e será capaz de estabelecer que a tal necessidade seja declarada formalmente.	Sim	Sim
Lista de acesso revisada pelo proprietário da área para evitar alterações não autorizadas.	Não	Sim com Revisão Mensal
A continuidade da necessidade de acesso de negócios declarada pelos indivíduos deverá ser verificada pelo proprietário da área.	Não	Sim com Revisão Mensal
Processo existente para revogação de acesso, por solicitação ou pela finalização do vínculo empregatício, deve ser analisado regularmente.	Não	Sim
Fazer revisões periódicas das áreas de processamento de dados e rever os logs de acesso para assegurar integridade e precisão.	Não	Sim

Localização de Componentes / Sistemas

Os requisitos de controle de acesso físico são aplicáveis à CPU, dispositivos conectados por canal e consoles masters e servidores/sistemas físicos (ou seja, dispositivos interativos que fornecem uma interface de comando ao sistema operacional sem a identificação e autenticação do operador). A área controlada utilizada baseia-se na importância do serviço de sistema que está sendo prestado e no valor do equipamento de processamento de informações.

Localização de Componentes de Instalações de Computação /Infra-estrutura de LANs	Área Mínima
Servidores	Sala trancada quando não há ninguém trabalhando
Pontes, Gateways, Repetidores, Roteadores, Switchs, Hubs e Gabinetes de cabeamento	Protegido
Modens	Sala trancada quando não há ninguém trabalhando

Nota:

As consoles do Sistema/Servidor localizadas em áreas Restritas ou Protegidas não precisam de proteção de senha ou senhas de inicialização.

- Chaves de sistemas não precisam ser removidas.

A responsabilidade por proteção de Salas externas ao Data Center é da infraestrutura e Segurança do **Grupo CPFL**.

Servidores LAN / Dispositivos de Infra Estrutura			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Proteger Servidores LAN e dispositivos de infra-estrutura nas instalações da DXC	**N/A**	**N/A**	**N/A**
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Proteger Servidores LAN e dispositivos de infra-estrutura nas instalações do **Grupo CPFL**	**A**	**E**	**-**

6.5. Controle de Acesso Lógico

Esta seção abordará diferentes aspectos de controle de acesso lógico. O acesso que está sendo controlado se refere a sistemas host ou LAN, a dados e privilégios do sistema.
Os controles de acesso lógico incluem os seguintes tópicos principais, e os Requisitos de cada um deles estão identificados nesta seção.

Identificar e Autenticar Usuários: Assegurar que um identificador único (ex: ID do usuário) possa ser associado a cada usuário potencial do sistema. Quando o usuário acessar o sistema, assegurar que um nível adicional de identificação (ex: uma senha) verifique se o usuário é quem ele alega ser.

Definir e Proteger Recursos: Assegurar que cada recurso no sistema possa ser identificado, que o acesso ao recurso possa ser permitido nos níveis apropriados para usuários autorizados e que o acesso possa ser negado a usuários não autorizados.

Administração do Sistema e de Segurança: Assegurar que apenas usuários autorizados possam definir, modificar, ou desativar as funções de segurança do sistema.

Registrar Tentativas de Acesso: Assegurar que possa ser criado um registro de auditoria para cada tentativa de acesso, bem ou mal-sucedida, ao sistema ou a recursos protegidos no sistema.

Relatar Violações de Acesso: Assegurar que tentativas não autorizadas de acesso aos sistemas ou informações possam ser reconhecidas como violações, e que tenha uma análise imediata ou subseqüente.

6.5.1. Identificar e Autenticar Usuarios

A autorização de acesso aos sistemas do **Grupo CPFL** deve ser baseada na necessidade de negócio, e deve ser verificada a identidade do usuário ou aplicativo. Os IDs do usuário devem ser identificáveis a uma pessoa pela atribuição de um ID do usuário único a cada pessoa e pela atribuição de um código secreto (ex. uma senha) conhecido apenas pelo proprietário do ID do usuário. Os IDs do usuário discutidos nesta seção são os utilizados para logon/login no sistema/servidor.

Nota:

- Em áreas de controle do centro de computação, IDs do usuário ou senhas de operações de sistemas podem oferecer acesso à funções que precisam ser utilizadas por um grupo de pessoas. Se a funcionalidade/utilidade do software não permitir que a responsabilidade individual seja mantida, os IDs do usuário ou senhas poderão ser compartilhados pelo grupo, de acordo com as seguintes condições:

Usuários compartilhados:

As seguintes especificações devem ser inclusas na implementação deste requisito, e aplicado somente a USERIDs DXC a menos que especificado no contrato.

- Usuários não devem ser compartilhados, a menos que a responsabilidade individual possa ser mantida.

    1. Controles técnicos para manter a individualidade devem ser usados se disponível.
    2. Se os controles técnicos não estiverem disponíveis, deve ser atribuído usuários individuais e se manter a individualidade.
    3. Se nenhuma das alternativas forem utilizadas para manter a individualidade, uma justificativa de negócio deve ser documentada.
    4. Guardar os documentos reconhecidos pelo **Grupo CPFL** durante o Contrato.
    5. Consultar as especificações técnicas das plataformas para mais detalhes específicos exigidos nos controles técnicos e processos.

- O uso não autorizado de usuário e/ou senha deve ser evitado.

- Os Ids podem ser compartilhados por membros de um mesmo grupo, se todos partilham uma mesma responsabilidade comum de trabalho.

- A propriedade de um ID compartilhado deve ser atribuído ao Líder do grupo. O proprietário é responsável para assegurar a individualidade do userid / senha compartilhada.

- O Usuário compartilhado não dever ser um ID que possa acessar as informações que o grupo não precisa saber.

- Usuários compartilhados não precisam ser removidos (deletados) desde que haja um processo de transferência quando termina a necessidade de negócio do proprietário.

- Quando a individualidade não pode ser mantida por controles técnicos, um inventário deve ser mantido para os usuários compartilhados e seus acessos privilegiados. No mínimo, o inventário deve incluir o usuário, o proprietário do usuário, a identificação única do dispositivo onde o usuário é compartilhado, e a lista de usuários que são autorizados a compartilhar o usuário/senha.

Usuários			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Realizar um inventário básico de IDs de usuários dos sistemas nos quais a DXC possui a responsabilidade pela segurança.	**E**	**E**	**-**
Realizar revisões periódicas dos acessos ao sistema de todos os funcionários **Grupo CPFL** e notificar à DXC sobre quaisquer alterações.	**A**	**E**	**-**
Estabelecer, alterar, desativar e remover IDs do usuário e autoridades de acesso associadas para funcionários da DXC (administrador de ID do usuário).	**E**	**A**	**-**
Responsabilidades Opcionais (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Estabelecer, alterar, desativar e remover IDs do usuário e autoridades de acesso associadas para funcionários do **Grupo CPFL** (administrador de ID do usuário).	**A**	**E**	**-**
Implementar e manter controles de segurança para os subsistemas e aplicativos que não utilizam software de controle de acesso para sua segurança.	**A**	**E**	**-**

Usuários	**Valor Sugerido**	**Acordado** Grupo CPFL
Permitir compartilhamento de IDs do usuário nas áreas de controle de centros de computação	Sim, com os controles acima	Sim, com os controles acima

Permitir compartilhamento de IDs do usuário nos andares das áreas de fabricação/testes	Sim, com os controles acima	Sim, com os controles acima

6.5.1.1. Autorização de Usuários

Deve ser implementado um processo para autorizar usuários para sistemas de computadores

Autorização de Usuários			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Autorização de IDs do usuário para o pessoal da DXC	**A**	**E**	**-**
Responsabilidades Opcionais (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Autorização de IDs do usuário para o pessoal do **Grupo CPFL**	**A**	**E**	**-**

Autorização de Acesso	**Valor Sugerido**	**Requerido** Grupo CPFL
Processo de Autorização	Notificar o gerente do usuário	Todos os chamados por aprovação do Superior Imediato, Gestor de Infra, Gestor de Sistemas e Gestor de Segurança.

6.5.1.2. Revogação de Acesso

Quando um usuário deixar a empresa, sair de licença sem expectativa de voltar ao emprego regular, ou deixar de ter uma necessidade de acesso válida, o responsável pelo usuário deverá notificar o administrador do sistema. O administrador do sistema deve ter um processo ou controle técnico para impedir o acesso do usuário:

- Os usuários privilegiados e usuários comuns tem que ter seus acessos removidos dentro dos SLAs definidos nos Processos Internos **Grupo CPFL** após a notificação do Gestor.

Revogação de Acesso

Revogação de Acesso			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Notificar o administrador quando algum funcionário DXC não precisar mais do acesso.	**E**	**A**	**-**
Optional Responsibilities (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Notificar o administrador quando algum funcionário **Grupo CPFL** não precisar mais do acesso.	**A**	**E**	**-**

6.5.1.3. Revisão de Vínculo Empregatício

Deve existir um processo periódico de verificação de vínculo empregatício (verificar se o usuário ainda é funcionário da empresa). Se o usuário não é mais funcionário, uma das seguintes ações deve ser tomada:

- O usuário deve ser removido do sistema
- O usuário deve ser revogado do sistema
- A senha do usuário deve ser alterada para um valor desconhecido para o ex-proprietário

Revisão de Vínculo Empregatício			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Realizar a revisão periódica de contas de usuários para os funcionários DXC	**E**	**-**	**-**
Responsabilidades opcionais (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Realizar a revisão periódica de contas de usuários para os funcionários **Grupo CPFL**	**A**	**E**	**-**

Revisão de Vínculo Empregatício Grupo CPFL	**Valor Sugerido**	**Requerido** Grupo CPFL
Frequência da revisão para funcionários **Grupo CPFL**	Anual	Prazos definidos nos Processos Internos **Grupo CPFL**

Evidência da execução da revisão e registro de ações corretivas	Reter a última revalidação executada	N/A, uma vez que não será executada para funcionários **Grupo CPFL**
Transferência de funcionários, mesmo que passem a não residir na mesma localidade, região ou país	Não necessitam ser removidos até que sua necessidade de acesso termine	N/A, uma vez que não será executada para funcionários **Grupo CPFL**

Revisão de Vínculo Empregatício DXC	**Valor requerido**
Frequência da Revisão de Vínculo Empregatício DXC	Anual com exceção dos Ambiente Críticos onde a revisão ocorrerá Trimestralmente

6.5.1.4. Revalidação de Necessidade de Negócio

Deve existir um processo periódico de revalidação de acessos dos usuários. Esta revalidação deve rever as contas dos usuários e acessos associados, e determinar se estes devem ser mantidos. Os acessos que deixarem de ser necessários devem ser reportados ao administrador do sistema para remoção imediata.

A revalidação pode ser executada utilizando-se um relatório enviado para o Gestor, contendo a relação dos funcionários com acesso ao sistema. O Gestor deve informar as discrepâncias ao Administrador do Sistema. Relatórios não precisam ser devolvidos.

Revalidação de Necessidade de Negócio para usuários			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Revalidação de Usuários DXC	**E**	**-**	**-**
Responsabilidades Opcionais (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Revalidação de usuários **Grupo CPFL**	**A**	**E**	**-**

Revalidação de Necessidade de Negócio para usuários	**Valor Sugerido**	**Requerido** Grupo CPFL

Frequência de Revalidação de Usuários **Grupo CPFL**	Anual	Prazos definidos nos Processos Internos **Grupo CPFL**
Frequência de Revalidação de Usuários DXC	Anual	Anual
Sistemas que são gerenciados como um cluster	Usuários precisam apenas ser revalidados para acesso aos sistemas do cluster e não para cada node do cluster	Usuários precisam apenas ser revalidados para acesso aos sistemas do cluster e não para cada node do cluster
Revalidação de usuários, Evidência de Conclusão (Usuários **Grupo CPFL**)	Reter a última revalidação executada	Executado conforme Processos Internos **Grupo CPFL**
Revalidação de usuários, Evidência de Conclusão (Usuários DXC)	Reter a última revalidação executada	Devem ser guardadas a revisão atual e a anterior

Revalidação de Necessidade de Negócio para usuários	**Valor requerido**
Frequência da Revisão de Necessidade de Negócio DXC	Anual **Ambientes Críticos – Trimestral**

6.5.1.5. Senhas

As senhas podem ser utilizadas para identificação básica de usuários. A solidez da senha é um fator fundamental na proteção de sistemas e aplicações. As regras de criação de senhas identificadas nesta seção são aplicáveis a todas as senhas utilizadas para verificar a identidade de usuários no acesso a sistemas e subsistemas.

Recomendações para Passwords	**Valor Sugerido**	**Requerido** Grupo CPFL
Comprimento mínimo da senha	8	Apendice InsightVM e Politicas **Grupo CPFL**

Sintaxe	Contém uma mistura de caracteres alfabéticos e não alfabéticos (números, pontuações ou caracteres especiais) ou uma mistura de pelo menos dois tipos de caracteres não-alfanuméricos	Contém uma mistura de caracteres alfabéticos e não alfabéticos (números, pontuações ou caracteres especiais) ou uma mistura de pelo menos dois tipos de caracteres não-alfanuméricos
Conter o userid do usuário na senha	Não	Não
Intervalo máximo para alteração (ver nota abaixo)	90 dias	Apendice InsightVM e Politicas **Grupo CPFL**
Idade mínima da senha	Para usuários compartilhados a idade mínima da senha pode ser inferior a um dia, ou 0, onde a responsabilidade individual é mantida por controles técnicos. Todos os outros usuários, terá a idade mínima definida no intervalo permitido pela plataforma, mas não menos de 1 dia	Para usuários compartilhados a idade mínima da senha pode ser inferior a um dia, ou 0, onde a responsabilidade individual é mantida por controles técnicos. Todos os outros usuários, terá a idade mínima definida no intervalo permitido pela plataforma, mas não menos de 1 dia
Número de mudanças de senhas nas quais as senhas não podem ser reutilizadas	6	Apendice InsightVM e Politicas **Grupo CPFL**
Compartilhamento de senhas	Sim, desde que sejam mantidos os controles	Sim, desde que sejam mantidos os controles da **seção 6.5.1**
Senha padrão que acompanham produtos de sistemas operacionais/programas para serem usadas durante a instalação do produto e do sistema	Alterar o mais rápido possível	Alterar o mais rápido possível
Senhas que não foram alteradas dentro do intervalo estabelecido, mas que estão em estado expirado	Não constitui violação do requisito de intervalo de alteração de senha	Não constitui violação do requisito de intervalo de alteração de senha

Nota: Usuários que não expiram a senha são permitidos para comunicação direta de sistema-para-sistema desde que as seguintes condições sejam satisfeitas:

- Logons interativos não são permitidos (por exemplo, logon individual no sistema) e privilégios não são atribuídos aos usuários.
- Se estas condições não forem atendidas, o seguinte controle do processo é necessário:
    1. Acesso à senha deve ser restrito apenas a administradores com uma necessidade de negócio.
    2. A responsabilidade individual deve ser mantida quando o logon interativo é necessário (isto é, um log deve ser mantido para gravação do indivíduo, usando a senha juntamente com um carimbo).
    3. A senha deve ser alterada quando o proprietário do ID do usuário ou qualquer pessoa com conhecimento da senha deixa o negócio, ou haja alterações na responsabilidade do trabalho**.**

6.5.1.6. Proteção de Senhas

Proteção de Senhas	**Valor Sugerido**	**Requerido** Grupo CPFL
Transmissão de Senha	Não devem ser transmitidas em formato texto simples pela Internet, redes públicas ou dispositivos sem fio	Não devem ser transmitidas em formato texto simples pela Internet, redes públicas ou dispositivos sem fio
Armazenagem de Senha	Devem ser encriptadas quando armazenadas em arquivos ou bases de dados. Se a Criptografia não for possível, o acesso deve ser restrito apenas aos administradores de segurança do sistema	Devem ser encriptadas quando armazenadas em arquivos ou bases de dados. Se a Criptografia não for possível, o acesso deve ser restrito apenas aos administradores de segurança do sistema

6.5.1.7. Tentativas de autenticação com senha errada

Devem ser implementados controles que limitem o número de tentativas consecutivas de autenticação com senha errada. Isto deve ser feito bloqueando ou revogando a conta do usuário, ou pela utilização de um “logon inductor” que incremente exponencialmente o tempo permitido entre painéis de “sign on”.

Tentativas de autenticação com senha errada	**Valor Sugerido**	**Requerido** Grupo CPFL
Número de tentativas consecutivas de autenticação com senha errada, que disparam o processo de bloqueio do logon do usuário	4	Apendice InsightVM e Politicas **Grupo CPFL**

6.5.1.8. Alteração de Senha

Deve ser implementado um processo para alteração de senhas. Este processo deve contemplar a identificação positiva do requerente (com base numa credencial), e a senha temporária deve ser enviada de forma segura para o requerente, o usuário principal, ou (em alternativa) o seu responsável direto.

Alteração de Senha			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Alteração de senhas de usuários DXC e entrega somente a pessoas autorizadas	**E**	**-**	
Estabelecer os critérios do processo de redefinição de senhas de usuários da DXC e divulgando-os as pessoas autorizadas (normal e surdos / deficientes auditivos como obrigatório)	**E**	**-**	**-**
Responsabilidades Opcionais (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Alteração de senhas de usuários **Grupo CPFL** e entrega somente a pessoas autorizadas	**A**	**E**	**-**
Estabelecer os critérios do processo de redefinição de senhas de usuários do **Grupo CPFL** e divulgando-os as pessoas autorizadas (normal e surdos / deficientes auditivos como obrigatório)	**A**	**E**	**-**

6.5.1.9. Aviso de Utilização de Negócio

O **Grupo CPFL** pode querer avisar aos indivíduos que o uso não autorizado de seus sistemas é uma violação dos direitos da empresa, bem como lembrar aos funcionários que os sistemas só podem ser utilizados para conduzir os negócios da empresa ou para fins autorizados pela administração da empresa.

Nota:

- Os administradores de sistema ou de segurança não são responsáveis por monitorar o sistema para detectar mau uso, está é uma responsabilidade dos gestores e dos funcionários. Os administradores de sistema e de Segurança acompanharão os gestores na execução destas atividades, se for solicitado.

- A obrigação de apresentar o aviso de utilização de negócio deve ser implementada somente se o sistema, subsistema ou aplicativo tiver um procedimento de logon direto, que tenha sido especificamente projetado para permitir que o administrador do sistema possa apresentar mensagens obrigatórias para os usuários durante o logon inicial.

Aviso de Utilização de Negócio	**Valor Sugerido**	**Requerido** Grupo CPFL
Conteúdo	Notificar os usuários de que o sistema deve ser utilizado apenas em atividades de negócio autorizadas pelo Gerenciamento do **Grupo CPFL**. Não utilizar frases como “Bem vindo ao ... ”	Esta notificação não é requerida.

6.5.2. Definir e Proteger Recursos

Objetos de dados (ou ativos) podem assumir a forma de texto, programas ou dados. Os objetos pertencentes a indivíduos ou grupos são ***recursos de usuário***. Os objetos que estão relacionados aos serviços ou funções do sistema são ***OSRs (Operating System Resources, ou recursos de sistema)***. Os OSRs são os dados que fazem parte de:

- Programas de controle do sistema e seus mecanismos de controle de acesso
- Subsistemas e produtos de programas

Definir e Proteger Recursos			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Instalar, manter e atualizar o software de controle de acesso existente, conforme a DXC julgar necessário para fornecer o serviço	**N/A**	**N/A**	**-**
Implementar funções e características do software de controle de acesso que satisfaçam as práticas de segurança do **Grupo CPFL**, conforme definido neste documento	**N/A**	**N/A**	**-**

6.5.2.1. Classificação de Objetos de Dados

A classificação de dados é a base legal e física para proteção contra perda, mal uso, divulgação não autorizada, etc.

Os administradores de sistema e de segurança não são responsáveis por assegurar que os proprietários obedeçam às normas de classificação de dados ou às exigências que são aplicáveis à marcação interna de classificação de segurança.

Classificação de Objetos de Dados	**Valor Sugerido**	**Requerido** Grupo CPFL
Classificação externa de objetos de dados (etiquetas)	Não requerido	Não requerido
Responsável pela classificação de objetos de dados quando os mesmos são criados	Proprietário do dado	Proprietário do dado

6.5.2.2. Proteção de Informação Confidencial

Os usuários e proprietários de recursos devem aderir ao nível de classificação suportado.

Proteção de Informação Confidencial			
Responsibilities (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Determinar o nível de classificação suportado pelos sistemas/servidores	**A**	**E**	**-**
Informar os usuários sobre a adequação dos sistemas/servidores ao armazenamento de informação confidencial.	**-**	**E**	**-**

Protecção de Informação Confidencial	**Valor Sugerido**	**Requerido** Grupo CPFL
Disponibilidade da informação confidencial	Somente a pessoas que possuem necessidade de negócio	Somente a pessoas que possuem necessidade de negócio
Acesso a informação confidencial	Explicitamente permitido a um usuário individual ou grupo	Explicitamente permitido a um usuário individual ou grupo
Pessoal de suporte ao sistema que executam atividades normais como backups de sistema	Não requer permissão de acesso explícita do usuário proprietário do recurso	Não requer permissão de acesso explícita do usuário proprietário do recurso
A transmissão de dados confidenciais pela Internet, redes públicas ou dispositivos sem fio	Criptografia	Utilização de criptografia restrita aos Ambiente Críticos conforme definido internamente pelo **Grupo CPFL**.

6.5.2.3. Recursos de Usuário

Os usuários e proprietários de recursos são responsáveis pelas opções de proteção definidas para os seus dados. Os administradores de sistema, ou de segurança, não são obrigados a validar as alterações do usuário às opções iniciais de proteção, nem a investigar a colocação de informação confidencial em recursos de usuário com acesso universal, ou inadequado.

Recursos de Usuário	**Valor Sugerido**	**Requerido** Grupo CPFL
Padrão inicial de opções de proteção de recursos de usuário	Limitar acesso ao proprietário do recurso	Limitar acesso ao proprietário do recurso

6.5.2.4. Recursos do Sistema Operacional

A integridade dos ***OSRs (Operating System Resources)*** deve ser garantida através da definição de opções adequadas de proteção.

Nota: Em auxílio à identificação das exceções mencionadas abaixo, o Manual de Implementação (InsightVM) se refere a todos estes recursos. Deverão ser incluídos nesta lista quaisquer recursos adicionais que requeiram controles especiais que tenham sido instalados localmente.

Recursos do Sistema Operacional			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Identificar os requisitos de proteção para os OSRs (recursos do sistema operacional para Servidores e Equipamentos Data Center)	**E**	**E**	
Implementar requisitos de proteção para os OSRs através de software de controle de acesso, utilizando o Processo de Controle de Mudanças/Alterações	**E**	**A**	**-**

6.5.2.5. Criptografia

As funções criptográficas convertem texto comum em texto cifrado, utilizando chaves criptográficas que podem variar no seu comprimento mediante o nível de segurança requerido. Tanto na criptografia simétrica (que faz uso de uma chave compartilhada entre os interlocutores) como na criptografia assimétrica (que faz uso de pares de chaves, pública e privada) deve existir um processo de gestão do

ciclo de vida das chaves criptográficas, que comporta criação, distribuição, validação, atualização, armazenamento, uso e expiração.

Se as chaves forem destruídas ou ficarem indisponíveis para as partes autorizadas, o processo de recuperação de informação deve permitir a recuperação da chave e da informação cifrada.

Criptografia			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Definir e fornecer à DXC os requisitos de criptografia do **Grupo CPFL**	**A**	**E**	**-**
Responsabilidades Opcionais (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Fornecer e suportar produtos de criptografia (ex. hardware e/ou software) conforme definido neste documento	**A**	**E**	**-**
Garantir a segurança e a distribuição das chaves de criptografia	**A**	**E**	**-**

6.5.2.6. Código Malicioso (Harmful Code)

Para prevenir a propagação de “harmful code” (código malicioso), recomenda-se a utilização de software antivírus.

Código Malicioso (Harmful Code)			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Fornecer e manter contratos de suporte para software de antivírus para os servidores do **Grupo CPFL** gerenciados pela DXC	**-**	**E**	**-**
Responder aos ataques de vírus e iniciar ação corretiva para eliminar os vírus detectados, assim como o efeito da sua atividade, nos servidores gerenciados pela DXC.	**E**	**A**	**-**
Responsabilidades Opcionais (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Identificar e implementar os requisitos de proteção para recursos residentes nas máquinas do usuário final	**-**	**E**	**-**
Manter as assinaturas de vírus atualizadas nas estações de usuários finais	**-**	**E**	**-**

Código Malicioso (Harmful Code)			
Executar auditorias das máquinas de usuário final potencialmente afetadas por vírus	**-**	**E**	**-**
Reagir a ataques de vírus e iniciar ação corretiva para eliminar os vírus detectados nas máquinas do usuário final	**-**	**E**	**-**

Código Malicioso (Harmful Code)	**Valor Sugerido**	**Requerido** Grupo CPFL
Intervalo de verificação com programa de antivírus	Pelo menos uma vez por semana	Pelo menos uma vez por semana
Atualização das assinaturas do programa antivírus	Pelo menos uma vez por dia se o acesso a rede estiver disponível. Se não houver acesso à rede, devem ser feitas atualizações de assinatura manuais, pelo menos uma vez por semana.	Pelo menos uma vez por dia se o acesso a rede estiver disponível. Se não houver acesso à rede, devem ser feitas atualizações de assinatura manuais, pelo menos uma vez por semana.

Caso um sistema seja infectado por um vírus de computador, o administrador do sistema deverá contatar o serviço apropriado no sentido de minimizar o dano causado pelo vírus.

6.5.3. Autoridade de Sistema e Autoridade de Administração Segurança

Os privilégios possibilitam o gerenciamento dos sistemas/servidores pelos usuários. Podem permitir um usuário definir ou alterar outros usuários, alterar definições de segurança de um sistema ou alterar componentes do sistema. Os privilégios não são para serem atribuídos aos usuários finais, devem ser restritos e controlados. Nas seções seguintes serão especificados como, quando atribuir, e como gerenciar os privilégios de um sistema ou de um servidor.

As seguintes autoridades são consideradas usuários com privilégios:

Autoridade de Sistema: Autoridade dada a um indivíduo através da designação de atributos, privilégios ou direitos de acesso associados a sistemas operacionais, para o desempenho de atividades de suporte e manutenção.

Autoridade Administrativa de Segurança: Autoridade dada a um indivíduo através da designação de atributos ou privilégios associados a sistemas de controle de acesso, para o estabelecimento e administração de controles de segurança de sistema.

Autoridade de Sistema e Autoridade de Adminsitarção de Segurança	
Inclusos:	Todos os usuários com privilégios definidos nas especificações técnicas
Especificações técnicas a serem excluídas:	NA

.

6.5.3.1. Administração

Deve ser implementado um processo que aprova e atribua privilégios.

Nota:

- O proprietário da autoridade privilegiada, o gerente do indivíduo, o gestor de sistemas e de segurança devem aprovar todos os pedidos antes de atribuir autoridades privilegiadas. A autorização pode ser feita de forma explícita ou através de demonstração de que os critérios para a necessidade do negócio foram satisfeitas.

- Usuários com autoridades privilegiadas devem ser revalidado por necessidade de negócio contínuo em uma base anual. O acesso é para ser revogado para todos os indivíduos cuja necessidade de negócio não satisfaçam os critérios definidos.

- Deve existir um processo de para remoção de autoridade, que atenda a remoção dentro dos SLAs definidos após a detecção ou a notificação de que a necessidade de um indivíduo de negócios tenha terminado.

- Autorizações para administração do sistema de segurança e administração de autoridades requer evidências de que o processo de revalidação anual foi realizado.

Administração de Privilégios			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Rever novos pedidos de autorizações privilegiadas de usuários	**-**	**E**	**-**
Aprovar novos pedidos de autorizações privilegiadas de usuários	**-**	**E**	**-**
Atribuir novos pedidos de autorizações privilegiadas de usuários	**E**	**-**	**-**

Administração de Privilégios			
Eliminar privilégios quando deixar de existir a respectiva autorização de gerência	**E**	**E**	**-**

Administração de Privilégios	**Valor Sugerido**	**Requerido** Grupo CPFL
Aprovação de autorizações privilegiadas	O proprietário da autoridade privilegiada	O proprietário da autoridade privilegiada, Gestor de Infra, Gestor de Sistemas e Gestor e Segurança.
Atribuição de autorizações privilegiadas	Aprovação antes da atribuição ou consistente com a descrição da função exercida (aprovação de autorizações privilegiadas)	Aprovação antes da atribuição ou consistente com a descrição da função exercida (aprovação de autorizações privilegiadas)
Userids do sistema com autorizações privilegiadas no suporte dos sistemas operacionais (máquinas de serviço, tarefas iniciadas, agentes, userids criados durante a instalação do sistema, etc.).	Podem estar associadas a um Departamento Cada pessoa que possa efetuar logon tem que ter uma necessidade válida	Podem estar associadas a um Departamento Cada pessoa que possa efetuar logon tem que ter uma necessidade válida
Autorizações privilegiadas implementadas através de acessos a grupos de usuários	Somente quando todos os membros do grupo têm uma necessidade de negócio válida, o privilégio é aprovado	Somente quando todos os membros do grupo têm uma necessidade de negócio válida, o privilégio é aprovado
Remoção de autorizações privilegiadas	Dentro do SLA definido após a detecção ou a notificação de que uma necessidade individual de negócios ou trabalho terminou.	Dentro do SLA definido após a detecção ou a notificação de que uma necessidade individual de negócios ou trabalho terminou.

6.5.3.2. Gestão

Deve ser implementado um processo que verifica periodicamente se os privilégios estão atribuídos somente a usuários autorizados. Esta atividade pode ser efetuada durante a Revisão de Segurança Lógica. Uma segunda possibilidade é ter um processo separado que efetue periodicamente uma revalidação de necessidade de negócio a usuários com autorizações privilegiadas.

Gestão de Privilégios			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Rever autorizações privilegiadas de usuários DXC	**E**	**A**	**-**
Revalidar a necessidade de negócio a usuários DXC com autorizações privilegiadas	**E**	**A**	**-**
Controlar e ser responsável pelos perfis de usuário Security Officer/Administrator em todos os sistemas (ex: Administrator em Windows, root em Unix) para os quais a DXC tem a responsabilidade de gestão de segurança	**E**	**A**	**-**
Responsabilidades Opcionais (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Rever os usuários privilegiados **Grupo CPFL**	**A**	**E**	**-**

Gestão da Autoridade de Sistemas e Autoridade de Administração de Segurança	**Valor Sugerido**	**Requerido** Grupo CPFL
Verificar autorizações privilegiadas para garantir que somente usuários autorizados detenham privilégios. Isto inclui os privilégios atribuídos a usuários ou a grupos	Durante a Revisão de Segurança (Security Review)	Durante a Revisão de Segurança (Security Review)
Revalidação das autorizações privilegiadas para assegurar que os usuários detenham uma necessidade de acesso aos sistemas	Anual	Anual **Ambientes Críticos – Trimestral**
Evidência da execução da revalidação de autorizações privilegiadas	Reter a última revalidação executada	Reter a última revalidação executada

Gestão da Autoridade de Sistemas e Autoridade de Administração de Segurança	Valor requerido
Frequência de Revalidação para usuários DXC	Annual Ambientes Críticos – Trimestral

6.5.4. Documentar Tentativas de Acesso

Como especificado no decorrer desta seção, os registros de logs que documentam o acesso a sistemas, recursos, ou funções especiais deverão ser mantidos para garantir a sua disponibilidade para análise posterior ou para serem utilizados durante a investigação de acessos não autorizados.

Nota: Nem todas as plataformas suportam o registro de log. Para identificar os sistemas que suportam o registro de log.

Documentar Tentativas de Acesso			
Funções/Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Capturar e manter os registros de acesso, por um período de retenção acordado mutuamente, e fornecer ao responsável do **Grupo CPFL** os relatórios dos registros retidos quando solicitado	**E**	**-**	**-**

Documentar Tentativas de Acesso	Valor Sugerido	**Requerido** Grupo CPFL
Retenção de registros de Log	60 dias	90 dias onde parte destas logs poderão estar armazenadas em Log Server ou haver a necessidade de restore do Backup para disponibilização.

6.5.4.1. Registros de Acesso ao Sistema

Registro de Acesso ao Sistema	Valor Sugerido	**Requerido** Grupo CPFL
Tentativas de Logon	Todas, bem ou mal sucedidas	Todas, bem ou mal sucedidas

6.5.4.2. Registro de Atividades

Registro de Atividades	**Valor Sugerido**	**Requerido** Grupo CPFL
Administração de Segurança ou do Sistema	Registro de comandos utilizados para alterar OSRs e o estado de segurança	Registro de comandos utilizados para alterar OSRs e o estado de segurança

6.5.4.3. Registro de Rede

Registro de Rede	**Valor Sugerido**	**Requerido** Grupo CPFL
Atribuição de endereço IP na rede (DHCP Server)	Registro de data, hora e IP	Não requerido
Liberação de endereço IP na rede (DHCP Server)	Registro de data, hora, IP, endereço MAC, nomes do domínio e do host	Não requerido

6.5.5. Reportar Violações de Acesso

6.5.5.1. Logons Inválidos

Deve ser implementado um processo para fornecer relatórios de tentativas de logon inválidos.

Logons Inválidos			
Funções/Responsabilidades Opcionais (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Fornecer relatórios de logons inválidos	**-**	**-**	-

Logons Inválidos	**Valor Sugerido**	**Requerido** Grupo CPFL
Disponibilidade de Relatórios	Por solicitação	Por solicitação

6.6. Monitoração de Segurança

Todos os sistemas devem ser submetidos a verificações periódicas de segurança (security review). Quaisquer desvios expressos nos resultados decorrentes do processo de verificação do estado de segurança devem ser corrigidos conforme indicado nas seções seguintes.

6.6.1. Revisão de Segurança Lógica

O processo de revisão de segurança deve ser conduzido em uma base periódica para verificar o status da segurança dos sistemas.
Deve existir um processo para executar as verificações de segurança nos sistemas e validar a conformidade com as especificações técnicas constantes no manual de implementação para os sistemas **Grupo CPFL**. A administração deve decidir sobre o nível da revisão de segurança (freqüência e escopo), com base no controle necessário para a conta ou dispositivo.

Revisão de Segurança			
Responsabilidades Opcionais (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Realizar a Revisão de Segurança a Sistemas	**A**	**E**	**-**
Executar ações corretivas para eliminar os desvios	**E**	**A**	**-**

Revisão de Segurança	**Valor Sugerido**	**Requerido** Grupo CPFL
Ambiente Críticos	Trimestral	Trimestral
Frequência para todos os demais sistemas	Semestral	Anual
Opções do sistema de controle de acessos	Verificar se as mesmas são estabelecidas em conformidade com o Manual de Implementação	Verificar se as mesmas são estabelecidas em conformidade com o Manual de Implementação (InsightVM)
Autoridade de sistema e administração de segurança	Assegurar que somente usuários aprovados possuem autoridade	Assegurar que somente usuários aprovados possuem autoridade
Programas de detecção de código malicioso	Verificar os programas necessários estão instalados e operacionais	Verificar os programas necessários estão instalados e operacionais

Registro de acesso e atividade	Verificar se existem	Verificar se existem
Evidência da execução da Revisão de Segurança	Reter a última execução	Reter a última execução
Desvios encontrados na Revisão de Segurança	Sempre que os desvios não puderem ser corrigidos dentro do tempo estipulado, tal fato deverá ser reportado à gestão do **Grupo CPFL** e da DXC.	Sempre que os desvios não puderem ser corrigidos dentro do tempo estipulado, tal fato deverá ser reportado à gestão do **Grupo CPFL** e da DXC.

6.6.2. Revisões de Atividades do Sistema

O gerenciamento e auditoria da DXC e do **Grupo CPFL** têm o direito de rever todos os registros de atividades do sistema para examinar qualquer evidência de abuso de autoridade.

6.6.3. Abuso de Autoridade

As pessoas as quais foram concedidos a autoridade de administração de segurança ou autoridade de sistema são colocadas numa função de confiança pela gerência. Esse nível de confiança não constitui a aprovação da gerência para operar fora dos controles de negócios estabelecidos. O abuso de autoridade é uma violação de confiança que não pode ser tolerada.

Se for detectada uma situação de abuso de autoridade a gerência deve tomar as medidas adequadas.

Abuso de Autoridade			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Tomar as medidas adequadas se o abuso de autoridade foi cometido por um funcionário do **Grupo CPFL**	**-**	**E**	**-**
Tomar as medidas adequadas, se o abuso de autoridade foi cometido por um funcionário da DXC	**E**	**-**	**-**

Abuso de Autoridade	**Valor Sugerido**	**Requerido** Grupo CPFL

Pessoas a serem notificadas caso algum problema sério de segurança seja descoberto pela Revisão de Segurança	Departamento de Segurança do **Grupo CPFL** e da DXC	Departamento de Segurança do **Grupo CPFL** e da DXC

6.6.4. Suporte a Auditoria Externa

As auditorias são conduzidas sob leis governamentais, certificação da indústria e requisitos de acionistas. O escopo de uma auditoria pode incluir tudo, desde a Segurança de TI a controles de negócios.

Suporte a Auditoria Externa			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Fornecer um ponto central de auditoria para definir controles de auditoria e coordenar atividades de auditoria da DXC	**E**	**-**	**-**
Fornecer um ponto central de auditoria para definir controles de auditoria e coordenar atividades de auditoria do **Grupo CPFL**	**-**	**E**	**-**
Fornecer suporte para atividades de auditoria da DXC, tais como a coleta de dados, instalação de ferramentas de auditoria e produção de relatórios	**E**	**E**	**-**
Desenvolver e implementar planos de ação da DXC para todos os resultados de auditoria que não forem compatíveis com este documento ou com o contrato	**A**	**E**	**-**

6.7. Gestão de Incidente de Segurança

Um incidente de segurança pode ter origem interna ou externa, pode envolver instalações físicas que não estejam sob a responsabilidade da DXC, e pode variar em severidade. Os incidentes de segurança na área de TI podem envolver entrada não desejada no sistema, destruição de dados, fraude, crime ou outros. Outros incidentes podem geralmente ser resolvidos pelo gerenciamento responsável pela instalação física.

Gestão de Incidente de Segurança

Gestão de Incidente de Segurança			
Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Informar imediatamente o coordenador para incidentes de segurança de qualquer problema de segurança e sugerir ação apropriada.	**E**	**E**	**-**
Responsabilidades Opcionais (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Coordenar e gerenciar a investigação de qualquer suspeita de incidente de segurança.	**A**	**E**	**-**

Gestão de Incidente de Segurança	**Valor Sugerido**	**Requerido** Grupo CPFL
Após a descoberta, ou suspeita, de um incidente, notificar	Representante de Segurança da DXC e do **Grupo CPFL**	Representante de Segurança da DXC e do **Grupo CPFL**
Coordenador de Incidentes	Criar um arquivo de registro (data, hora e origem) para identificar cada informação relacionada com o evento.	Criar um arquivo de registro (data, hora e origem) para identificar cada informação relacionada com o evento.
Administrador do Sistema	Conter ou diminuir o dano a ativos e dados	Conter ou diminuir o dano a ativos e dados

Depois de detectado um incidente, os funcionários da DXC seguirão as orientações abaixo, salvo indicação contrária do coordenador de incidentes de segurança:

- Não tentar executar uma investigação ou "limpeza" do sistema.
- Manter sigilo sobre a investigação na estrita base da "necessidade de conhecimento".
- Não contatar pessoas ou organizações que sejam suspeitas de ser a origem do incidente. A DXC não comunicará com nenhuma entidade em nome do **Grupo CPFL**.

6.8. Processo de Alerta de Segurança/Integridade

Um Alerta de Segurança/Integridade é um aviso em relação a uma exposição num programa ou processo que permite a usuários não autorizados obter privilégio de autoridade num sistema, contornar o sistema de controle de acesso, ou obter acesso não autorizado à informação. Para instalar as correções (fixes/patches) deve ser seguido um Processo de Alerta de Segurança/Integridade. Os principais requisitos neste processo são:

- Determinação da severidade do risco, com base na classificação da vulnerabilidade e categoria de exploração.
- Notificação de disponibilidade de correções.
- Procedimento para determinar a programação da aplicação dos fixes de segurança/integridade.
- O Processo é auditado.

Processo de Alerta de Segurança/Integridade			
Funções/Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Notificar o **Grupo CPFL** quando uma correção com implicações de segurança ou integridade se tornar disponível.	**E**	**E**	**-**

6.8.1. Severidade

Podem ser atribuídas diferentes níveis de severidades aos Alertas de Segurança/Integridade, que serão utilizados na determinação do prazo de implementação. Os critérios utilizados para atribuição do nível de severidade são:

Classificação da Vulnerabilidade:

Alta: Burlar os controles de acesso do sistema ou obter acesso a um userid que possua autoridade de administração de sistema, ou de segurança, sem necessitar de um userid de usuário geral.

Média: Burlar os controles de acesso do sistema ou obter acesso a um userid que possua autoridade de administração de sistema, ou de segurança, utilizando um userid de usuário geral existente, ou ter acesso não autorizado a informação sem necessitar de um userid de usuário geral.

Baixa: Acesso não autorizado a informação utilizando userid de usuário geral ou um ataque de negação de serviço.

Categoria de Exploração:

Alta: A vulnerabilidade pode ser explorada por um usuário com nível de conhecimento básico para contornar os controles de acesso de forma intencional ou não intencional. Não é necessário conhecer nem o sistema operacional nem o ambiente. Exemplo: seguir um script simples.

Média: A vulnerabilidade pode ser explorada por um usuário com nível de conhecimento intermédiario, para burlar os controles de acesso de forma intencional ou não intencional. Requer o conhecimento da interface de nível de comando com o sistema operacional ou ambiente.

Baixa: A vulnerabilidade pode ser explorada por um usuário com nível de conhecimento avançado para contornar os controles de acesso de forma intencional ou não intencional. São necessários níveis de

conhecimento de especialista ou desenvolvimento de produtos para utilizar a interface de nível de comando com o sistema operacional ou ambiente.

Classificação de Severidades para Alertas de Segurança/Integridade			
Categoria de Exploração	**Alta Vulnerabilidade**	**Média Vulnerabilidade**	**Baixa Vulnerabilidade**
Alta Exploração	Alta	Alta	Média
Média Exploração	Alta	Média	Baixa
Baixa Exploração	Média	Baixa	Baixa

6.8.2. Plano de Notificação

Quando uma correção de Segurança/Integridade estiver disponível, a DXC e o **Grupo CPFL** realizam a classificação de severidade.

6.8.3. Plano de Implementação

Uma vez notificado, um plano da implementação de Alertas de Segurança/Integridade será definido por meio de acordo e a equipe DXC de implementação, seguindo o Processo de Alterações. O plano deve considerar:

- O teste, se desejado
- A indisponibilidade dos sistemas para os quais as correções terão que ser aplicadas afim de assegurar que não haverá interrupção nos processos críticos de negócio, a menos que haja acordo prévio
- O número de sistemas nos quais serão aplicadas correções

Nota: Um planejamento pode não incluir a instalação de um fix em todos os sistemas ao mesmo tempo. O plano pode especificar a mesma data, ou datas diferentes, desde que acordadas por ambas as partes.

Plano de Implementação

Plano de Implementação			
Funções/Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Acordar o plano de implementação para os fixes identificados	**A**	**E**	**-**
Obter e aplicar os fixes de Segurança/Integridade dentro do tempo acordado	**E**	**A**	**-**

Plano de Implementação	**Valor Sugerido**	**Requerido** Grupo CPFL
Retenção as Evidências de Patch Management e Vulnerability	Reporte Mensal	Reporte Mensal

Plano de Implementação – Ambiente Distribuído e SQL

Severidade	**Valor Sugerido**	**Requerido** Grupo CPFL
Alta Severidade	30 dias	30 dias
Média Severidade	60 dias	60 dias
Baixa Severidade	90 dias	90 dias

Plano de Implementação – Oracle

A implementação dos Patches Oracle, serão realizados a cada 180 dias, ou seja, 2 vezes ao ano devido a complexidade do Ambiente.

A Oracle libera os patches 4 vezes ao ano (JANEIRO, ABRIL, JULHO e OUTUBRO).

Patches	**Valor Sugerido**	**Requerido** Grupo CPFL
Patches Oracle	180 dias	180 dias

Plano de Implementação – UNIX

Severidade	**Valor Sugerido**	**Requerido** Grupo CPFL

TL	365 dias	365 dias
Service Pack	90 dias	365 dias
APAR	Conforme necessidade	Conforme necessidade

Plano de Implementação – SAP

Tipo de Correção	**Valor Sugerido**	**Requerido** Grupo CPFL
Aplicação de Nota	Conforme necessidade do sistema.	Diante de solicitação do **Grupo CPFL** /Funcional SAP.
Suporte Package	Conforme necessidade do sistema.	Diante de solicitação do **Grupo CPFL**/Funcional SAP.
Atualização de Kernell	180 dias	180 dias

Patches Zero Day – aplicação imediata

6.9. Segurança de Aplicações/Usuário Final

6.9.1. Segurança de Aplicações

A segurança dos programas e dados associados às aplicações deve ser protegida de acesso ou uso não autorizado. Para este efeito, devem ser obtidas as seguintes especificações junto do proprietário da aplicação:

- Qual o acesso público a programas e dados
- Lista de usuários que necessitam de acesso adicional a programas e dados
- Requisitos de log auditado para programas e dados

Não será feita qualquer alteração à proteção de programas ou dados sem a aprovação do proprietário da aplicação.

Segurança de Aplicações

Segurança de Aplicações			
Responsabilidades Opcionais (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Definir os requisitos de proteção para os recursos de aplicações através do Software de Controle de Acesso	**A**	**E**	**-**
Implementar os requisitos de proteção para os recursos de aplicações através do Software de Controle de Acesso (quando o controle for feito através da aplicação)	**A**	**E**	**-**

6.9.2. Segurança de Usuário Final

Segurança de Usuário Final			
Funções/Responsabilidades Opcionais (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Definir os requisitos de proteção para os dados do usuário final através do Software de Controle de Acesso	**-**	**E**	**-**
Implementar os requisitos de proteção para os recursos do usuário final através do Software de Controle de Acesso	**A**	**E**	**-**
Responsabilidade pela proteção dos dados classificados	**A**	**E**	**-**

Segurança de Usuário Final	**Valor Sugerido**	**Requerido** Grupo CPFL
Recurso contendo informações não classificadas	O proprietário do recurso pode alterar explicitamente, a proteção de acesso padrão	O proprietário do recurso pode alterar explicitamente, a proteção de acesso padrão

6.10. Controles de Rede

6.10.1. Acesso à Rede de Dados

O acesso ao software que monitora, manipula ou modifica as configurações ou dispositivos associados na rede local deve ser controlado para impedir interferência não autorizada.

As informações sobre software de controle de rede estão documentadas no Manual de Implementação.

Acesso à Rede de Dados			
Funções/Responsabilidades (E = Executor, A = Auxiliar)	**DXC**	Grupo CPFL	**N/A**
Gerenciamento e manutenção dos componentes de infraestrutura de rede que podem se conectar à rede **Grupo CPFL** e da DXC a fim de fornecer o serviço.	**E**	**E**	**-**

Acesso à Rede de Dados	**Valor Sugerido**	**Requerido** Grupo CPFL
Acesso ao software de gestão de rede	Limitado a pessoas cuja responsabilidade inclua suporte à rede	Limitado a pessoas cuja responsabilidade inclua suporte à rede
Revalidação de Acessos	Anual	N/A pois apenas os usuários da Equipe de Redes deverão ter o acesso privilegiado aprovado.
Atributos ou privilégios que permitam modificação ou manipulação das configurações ou dispositivos da rede	Tratados como autoridade de administração de segurança	Tratados como autoridade de administração de segurança

7. CONTROLE DE REGISTROS

Identificação	**Armazenamento e Preservação**	**Proteção (acesso)**	**Recuperação e uso**	**Retenção**	**Disposição**
Ocorrências Relatórios Ata de Reunião	Diretório Software DR	Backup, Antivirus, Restrição de Acesso	Backup Replica DR	Poltica de Backup e Normas	Deletar

8. ANEXOS

Não aplicável

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
DXC	Segurança da Informação	Daniela Saran
CPFL	Governança CPFL	Heliane Pontes

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
x	24/03/2010	Criação do documento
x	18/05/2010	Assinatura
x	19/07/2010	Alteração de Data de Revisão – ambiente SOX, alterações no Processo de Security Review, Acesso ao Data Center.
x	04/11/2011	Alteração de Data de Revisão – ambiente SOX, alterações no Processo “Userid Revalidation of Continued Business Need”, “Employment Review” e “Invalid Password Attempts” (alteração de parâmetro) e atualização dos ambientes SOX.
x	07/03/2012	Revisão geral do documento
x	18/02/2013	Padronização de Acesso Fisico ao Data Center e acerto de data para Revalidação de Vinculo Empregaticio (QEV) para funcionários DXC/Service
x	16/12/2013	Padronização de aplicação de patches/fixes de Segurança
x	23/06/2015	Revisão geral do documento
x	18/01/2016	Alteração do repositório de apêndices
x	01/03/2016	Revisão geral do documento - Padrão CPFL e publicação no GED
1.0	28/02/2018	Revisão Geral do documento
1.1	02/03/2018	Revisão geral do documento e adequação ao modelo para elaboração de documentos no GED.
1.2	01/04/2022	Revisão geral do documento
1.3	29/04/2022	Inclusão da Definição “Grupo CPFL”