Universidade São Judas Tadeu

Eduardo Cecilio Alves Santos – RA:824224719

Projeto A3 - UC Ambientes Computacionais e Conectividade

Estudo De Caso 2

São Paulo

2025

1. A política da ATI sobre o uso da Web parece dura para você? Por que ou por que não?

R:Depende.

Do ponto de vista da segurança da informação:

Não é dura, é prudente. Muitas organizações, especialmente aquelas que lidam com dados sensíveis ou estão em setores regulados (como finanças, saúde ou consultoria), precisam de **controle rígido sobre o uso da internet** para:

Evitar vazamento de informações.

Proteger contra malware hospedado em sites desconhecidos.

Garantir produtividade e conformidade com normas internas.

Do ponto de vista do funcionário:

Pode parecer **rígida ou inflexível**, especialmente se aplicada sem contexto ou com pouco espaço para exceções. O bloqueio total de sites com imagens, por exemplo, pode afetar profissionais que realmente precisem acessar esse conteúdo para fins de trabalho legítimos.

A política é justificada tecnicamente, mas deve ser comunicada com clareza, revisada periodicamente e aplicar exceções de maneira razoável.

2. Você acha que Ron foi justificado em suas ações?

R:Sim e não.

Sim (humanamente falando):

Ele terminou um projeto desgastante, estava no final do expediente e buscava algo inofensivo (férias).

Isso mostra a **necessidade de pausas e equilíbrio** — algo que gestores e RHs deveriam considerar.

Não (do ponto de vista da política da empresa):

Ele sabia que a empresa tinha um servidor proxy e que o acesso irrestrito não era permitido.

Ignorar uma política intencionalmente, mesmo que por um bom motivo, ainda é uma violação**.**

Portanto Ron teve uma motivação compreensível, mas a ação foi um desvio das normas estabelecidas. O ideal seria pedir liberação prévia ou usar dispositivos pessoais fora da rede corporativa.

3. Como Andy deve reagir a essa situação se Ron é conhecido por ser um funcionário confiável e diligente?

R:Andy deve equilibrar **empatia** com **responsabilidade corporativa**. Uma abordagem recomendada seria:

a) **Conversa direta e respeitosa:**

Andy deve conversar com Ron em particular, reconhecer seu bom trabalho e questionar sua visão sobre o ocorrido. Algo como:

"Ron, vi a notificação do time de segurança. Sei que você tem trabalhado duro e que todos precisamos de um respiro às vezes, mas precisamos conversar sobre isso."

b) **Ajudar a mitigar as consequências:**

Se Andy considerar que não houve má-fé, pode **interceder com o setor de segurança** para restaurar os privilégios de rede de Ron o quanto antes.

Pode sugerir o curso de uso adequado da internet como algo **preventivo e não punitivo**.

c) Reforçar a política, mas com abertura:

Andy pode usar a oportunidade para reforçar que as políticas existem por um motivo, mas também pode:

Propor melhorias na política (como uma "janela recreativa", ou acesso limitado durante pausas).

Criar um processo mais ágil para solicitar acesso temporário a sites legítimos.