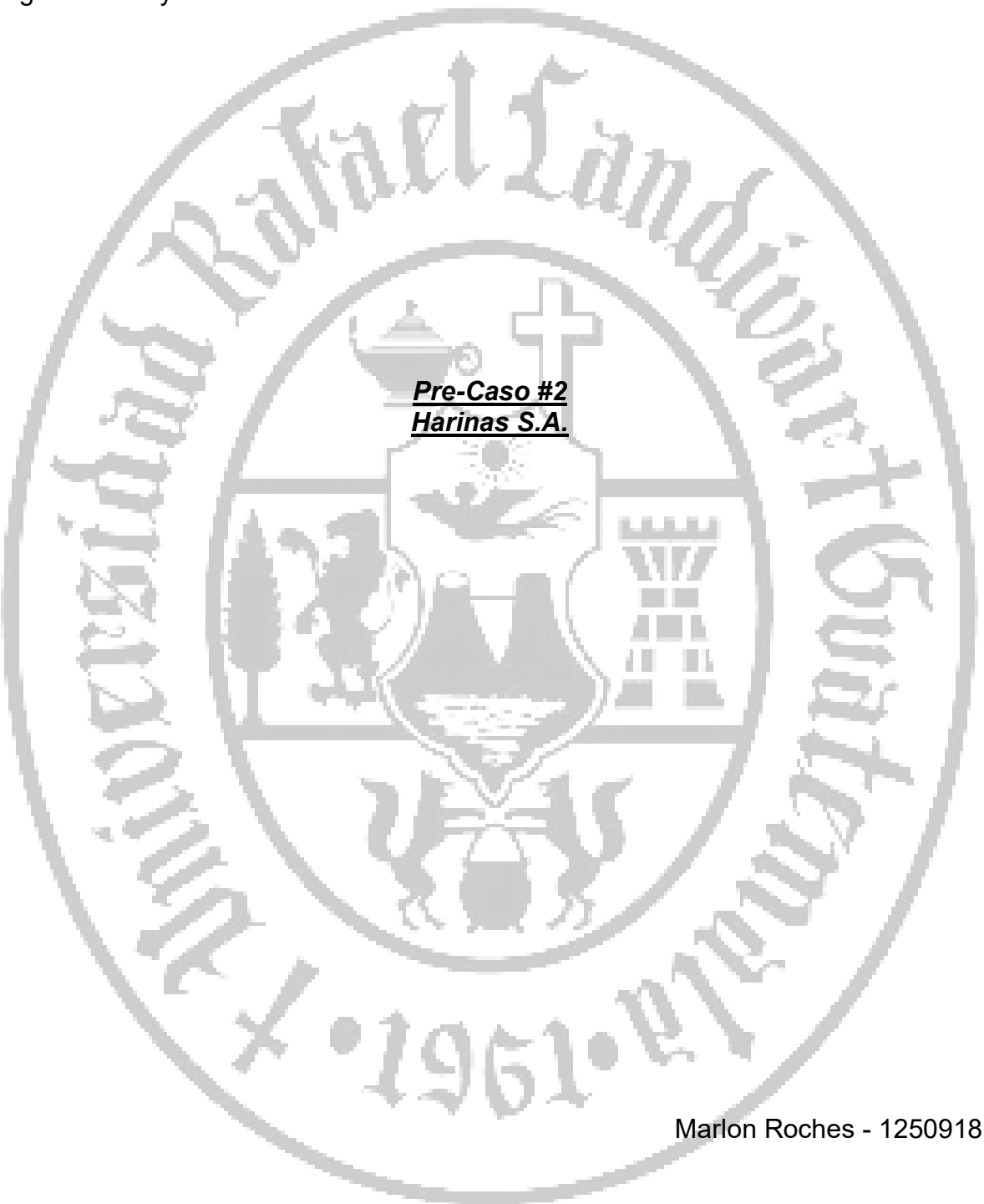
Universidad Rafael Landívar
Facultad de Ingeniería
Sección: 01
Ing. David Reyes



Pre-Caso #2
Harinas S.A.

Marlon Roches - 1250918

Guatemala de la Asunción 13 de abr. de 23

Introducción

El caso de Harinas S.A. presenta un escenario en el que la empresa, dedicada a la producción de pan y pasteles de calidad "premium" en 30 plantas ubicadas en América, ha sido afectada por problemas de adquisición de materias primas y, como resultado, se han manifestado diferentes afecciones en cada planta descentralizada, incluyendo problemas en los sistemas de información. En particular, una de las plantas ubicadas en Guatemala ha solicitado la intervención de profesionales en tecnología para resolver los problemas que afectan su operación, lo que puede tener implicaciones en todas las plantas de la empresa. Los problemas incluyen la elusión de las normativas de navegación por parte de los usuarios, fallas constantes en los sistemas de información, incapacidad para reparar equipos con agilidad, introducción de dispositivos USB infectados, compartición de credenciales de puntos de red inalámbricos, almacenamiento de información personal en equipos laborales, entre otros.

Resumen ejecutivo del pre-caso

La empresa multinacional Harinas S.A. está experimentando problemas de adquisición de materias primas y ha identificado a través de una planta en Guatemala diferentes problemas de tecnología que afectan a varias plantas en América. Los problemas incluyen la evasión de normativas de navegación implementadas por IT, altas demandas de reparación de equipos, la introducción de dispositivos USB infectados, la compartición de credenciales de red inalámbrica y prácticas inadecuadas por parte de los usuarios. Además, la gerente general está preocupada por el aumento de las vulnerabilidades informáticas. Se solicita a un profesional del área de tecnología que proponga soluciones para abordar estos problemas.

Resolución de los cuestionamientos

¿Qué haría para resolver el caso?

como profesional del área de tecnología de la información, propondría un enfoque de solución integral que aborde cada uno de los problemas identificados y que promueva la colaboración entre los departamentos y la estandarización de procesos y herramientas en todas las plantas de la empresa.

Primero, se debería implementar una política clara y rigurosa de seguridad de la información, que incluya la gestión de contraseñas, la limitación del acceso a sitios no autorizados, la implementación de herramientas de prevención de virus y la realización de auditorías de seguridad regulares.

En segundo lugar, se debería establecer un sistema de gestión de activos de tecnología de la información para controlar y optimizar el uso de los recursos, incluyendo la asignación de equipos y dispositivos a los empleados y la programación de mantenimiento preventivo para evitar fallas frecuentes.

Por último, se debería establecer un programa de capacitación y concientización para los empleados, que promueva una cultura de seguridad de la información y un uso responsable de los recursos tecnológicos de la empresa.

En general, la solución propuesta se basa en la estandarización de procesos y herramientas en todas las plantas de la empresa, lo que permitiría una mayor eficiencia y reduciría los riesgos de seguridad.

¿Porqué lo haría de esa forma?

La estrategia propuesta se basa en abordar los problemas de forma integral y sistemática, considerando tanto la tecnología como los aspectos culturales y de comunicación dentro de la empresa. Se busca fomentar una cultura de responsabilidad y compromiso por parte de los empleados, al mismo tiempo que se implementan medidas tecnológicas efectivas para garantizar la seguridad y el buen uso de los recursos informáticos.

Se opta por la implementación de una plataforma de educación y concientización sobre seguridad informática para los empleados, que incluya cursos interactivos y material informativo sobre buenas prácticas y riesgos a los que se exponen al no seguir las políticas establecidas por la empresa. Además, se propone una revisión y actualización de las políticas de seguridad de la información y el fortalecimiento de los controles de acceso y monitoreo en la red.

Para el tema de la alta demanda de reparaciones de equipos informáticos, se propone establecer un servicio de atención al usuario con un sistema de tickets para la gestión de solicitudes de reparación, priorizando las fallas más críticas y estableciendo tiempos de respuesta definidos.

También se propone la implementación de medidas de seguridad adicionales, como la implementación de un sistema de control de dispositivos USB, el establecimiento de credenciales individuales para los puntos de red inalámbricos y la adopción de un software de monitoreo de actividades de la red.

Por último, se propone la creación de un plan de contingencia y recuperación ante desastres, para prevenir y manejar situaciones de vulnerabilidad informática.

¿Cómo resolvería empleando los recursos propuestos?

Se pueden emplear los siguientes recursos:

1. Implementación de políticas y capacitaciones: Es necesario implementar políticas claras de uso de tecnología en la empresa y capacitar a los empleados para que comprendan su importancia y las consecuencias de no seguirlas. Esto incluye normativas de navegación en internet, uso de dispositivos USB, manejo de contraseñas, entre otros aspectos.

2. Actualización de equipos y software: Es importante actualizar los equipos de IT para que puedan atender de manera más ágil y efectiva las solicitudes de los usuarios. Además, se deben actualizar los programas de seguridad y antivirus para asegurar una protección adecuada.

3. Implementación de medidas de seguridad en la red inalámbrica: Se debe configurar la red inalámbrica para que los usuarios no puedan compartir las credenciales y se deben crear redes inalámbricas separadas para los dispositivos personales.

Conclusiones

En conclusión, la resolución del caso de Harinas S.A. implicaría la implementación de medidas y soluciones en varios aspectos, incluyendo la seguridad informática, la gestión de los equipos y dispositivos, el uso de recursos y la cultura organizacional.

Para abordar estos problemas, se debe comenzar con la formación de una cultura de conciencia de seguridad informática y el establecimiento de políticas claras para el uso de recursos y dispositivos. Además, se deben implementar medidas técnicas, como el fortalecimiento de los sistemas de antivirus y firewall, la actualización de los equipos, la implementación de un sistema de gestión de inventarios de hardware y software y el uso de herramientas de control de acceso y monitoreo de tráfico.

También se debe considerar la externalización de algunas de las funciones de IT, como el soporte técnico de nivel 1, para liberar a los técnicos de IT internos de las tareas cotidianas y permitirles enfocarse en problemas más críticos.

Anexos (Diagramas)

Recomendaciones

Implementar políticas claras y comunicarlas a los empleados: es importante establecer políticas claras para el uso de los recursos informáticos y de tecnología en la empresa. Estas políticas deben ser comunicadas y explicadas claramente a todos los empleados para asegurar su cumplimiento.

Realizar capacitaciones y entrenamientos periódicos: para garantizar que los empleados estén al tanto de las políticas y procedimientos de seguridad informática y de tecnología, se deben realizar capacitaciones y entrenamientos periódicos. De esta manera, los empleados estarán mejor preparados para prevenir y evitar riesgos informáticos.

Implementar soluciones tecnológicas: la implementación de soluciones tecnológicas como firewalls, antivirus, software de monitoreo y control de acceso pueden ayudar a reducir los riesgos informáticos. Además, se deben establecer controles de acceso a la red inalámbrica y limitar la cantidad de dispositivos que pueden conectarse a la red.