Universidad Nacional de Tucumán

Facultad de Ciencias Económicas

Seguridad y Control en Sistemas Informáticos

CONCIENTIZACIÓN EN SEGURIDAD INFORMÁTICA EN UNA PYME:

ESTRATEGIAS DE BAJO COSTO PARA REDUCIR VULNERABILIDADES

CERVIÑO, JULIETA CAMILA **- CORONEL,** MARIA VICTORIA **- FONTS,**

SOLANA MARÍA **- RODRÍGUEZ LIEB,** SOFIA

2024

DECLARACIÓN JURADA DEL ORIGEN DE LOS CONTENIDOS

"Por medio de la presente, los autores manifiestan conocer y aceptar el "Reglamento para la Presentación de Trabajo Final" vigente de la asignatura "Seguridad y Control en Sistemas Informáticos", haciéndose responsables por la totalidad de los contenidos del presente documento, los cuales son originales y de creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación nacional e internacional de Propiedad Intelectual".

Cerviño, Julieta Camila

Coronel, Maria Victoria

Fonts, Solana María

Rodriguez Lieb, Sofia

FIRMADO

RESUMEN

En un contexto de crecientes amenazas cibernéticas, las pequeñas y medianas empresas (Pymes) también enfrentan vulnerabilidades críticas que pueden afectar su operatividad y reputación. A partir de esto, este trabajo evalúa el nivel de concientización y prácticas de seguridad informática en una Pyme tucumana dedicada a la producción de snacks salados, identificando sus vulnerabilidades y su percepción sobre riesgos informáticos. A partir de la realización de una entrevista al dueño de la empresa, un análisis de sus prácticas actuales y su contexto, se diseñó un plan de acción accesible y de bajo costo para que, de esta manera, esta organización pueda implementar la seguridad de la información en sus procesos de manera exitosa.

Se proyecta que, al implementar estas medidas, la empresa reduciría incidentes de

seguridad y fortalecería su cultura organizacional en ciberseguridad y su ciber-resiliencia, otorgando beneficios operativos y de protección de datos para la realización de sus procesos.

Este estudio destaca la importancia de la implementación de prácticas de ciberseguridad en Pymes y ofrece recomendaciones adaptables a recursos limitados.

Palabras Clave: Seguridad Informática - Pyme - Concientización - Plan - Riesgos.

TABLA DE CONTENIDOS

INTRODUCCIÓN

Las pequeñas y medianas empresas (Pymes) son un motor clave en la economía regional, enfrentando tantas oportunidades como desafíos específicos para su crecimiento y continuidad. En este contexto, la seguridad de los sistemas informáticos se vuelve esencial para garantizar la protección de los datos y la eficiencia de los procesos internos. Este trabajo se centra en una Pyme tucumana dedicada a la producción y comercialización de snacks de alta calidad, la cual, a través de una cadena de producción vertical, ha logrado posicionarse en el mercado regional y expandir su alcance a varias provincias. Sin embargo, como muchas otras Pymes en expansión, enfrenta riesgos y vulnerabilidades en sus sistemas informáticos. En este estudio, se examinan las prácticas de seguridad actualmente implementadas en la organización, con el objetivo de diseñar un plan de concientización y recomendaciones según las necesidades de la organización. Este plan busca fortalecer la cultura de seguridad de la información dentro de la empresa, subrayando su importancia para la continuidad y la reputación del negocio.

PLANIFICACIÓN DE LA INTERVENCIÓN Y DE SU SEGUIMIENTO

OBJETIVO DEL PRESENTE TRABAJO:

El objetivo de este trabajo es evaluar el nivel de concientización y las prácticas de seguridad informática en una Pyme tucumana. A través de un diagnóstico que incluye observaciones directas y una entrevista al dueño de la empresa, y con apoyo en un marco teórico centrado en temas de ciberseguridad y protección de datos, se busca identificar las vulnerabilidades existentes en sus sistemas informáticos y entender cómo la empresa percibe los riesgos informáticos. Con base en estos hallazgos, se propone un plan de concientización de bajo costo que muestre la importancia de implementar sistemas de seguridad para reducir

vulnerabilidades, gestionar riesgos y fomentar una cultura de seguridad informática en toda la empresa, lo que también permitirá la continuidad operativa de la empresa ante ciberataques.

ALCANCE DEL TRABAJO

El alcance de este trabajo incluye un análisis exhaustivo de las prácticas de seguridad informática actualmente implementadas en las Pyme, con un enfoque en los riesgos específicos de ciberseguridad que enfrentan las pequeñas y medianas empresas en expansión. El trabajo se desarrolla mediante métodos como entrevista y observación detallada de las prácticas de seguridad aplicadas, con el propósito de adaptar las recomendaciones a las necesidades y limitaciones de la organización. Además, se diseñará un plan de concientización personalizado para fortalecer la cultura de seguridad de la información dentro de la empresa, mejorando la protección de sus datos y preservando su reputación en el mercado.

ÁMBITO DE DESARROLLO

El desarrollo del trabajo se centra en el análisis de la seguridad informática dentro del entorno específico de la empresa planteada. Esto incluye el entorno organizacional interno, explorando sus sistemas informáticos, sus prácticas actuales de seguridad, y la percepción y concientización de los empleados y directivos sobre los riesgos informáticos. También considera el entorno de riesgos informáticos comunes en las Pymes, teniendo en cuenta los desafíos que enfrentan estas empresas en términos de presupuesto y recursos limitados para la seguridad. Por último, el ámbito de intervención abarca un plan de concientización y recomendaciones que respondan a las necesidades de la empresa, favoreciendo no solo la mejora técnica, sino también el fortalecimiento de una cultura organizacional orientada a la seguridad de la información.

INTERVENCIÓN

Para recolectar datos utilizamos un **método cualitativo**, específicamente con la herramienta de la entrevista y la observación directa.

En la entrevista realizada, se abordan temas acerca de la implementación de seguridad de la información en los procesos de la empresa, su conocimiento y opinión al respecto.

La empresa cuenta con un sistema de información tercerizado, brindado por "**Infomanager"**, el cual es un sistema de gestión empresarial más simple y flexible que SAP (sistema por el que la empresa está considerando cambiar). Suele ser elegido por empresas que se encuentran en etapas iniciales o que necesitan una solución más ligera y económica para manejar datos. Aunque Infomanager permite gestionar ciertos procesos básicos, generalmente es menos robusto en términos de seguridad, controles avanzados y funciones integradas de auditoría que SAP. Este último podría proporcionar funciones más completas de monitoreo y protección de datos, además de integrarse con herramientas de ciberseguridad y gestión de accesos que ayudan a proteger los activos críticos de la empresa. Por otro lado, cuentan con conectividad a través de wifi satelital y uso de nube.

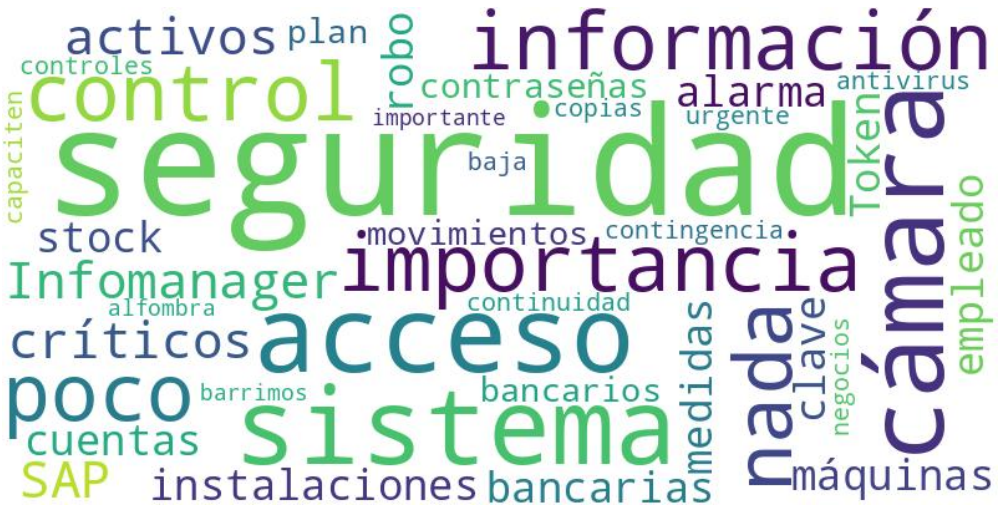
También, identifican como activos críticos sus productos terminados, maquinaria, terrenos, instalaciones y cuentas bancarias, pero su protección es limitada. A raíz de un robo interno, instalaron cámaras y alarmas en depósitos y oficinas. Para la seguridad bancaria, dependen de medidas ofrecidas por el banco, como el uso de contraseñas y claves token, aunque estas credenciales están en manos de cuatro personas, una situación que reconocen debe ajustarse.

No cuentan con un plan de continuidad de negocios y mencionan que, en caso de incidente, no tienen una respuesta clara ni establecida. La baja de accesos al sistema se realiza

manualmente tras la salida de empleados, lo que podría permitir vulnerabilidades. Tampoco disponen de antivirus y las copias de seguridad se realizan de forma esporádica y sin control de consistencia entre los empleados.

Finalmente, el entrevistado expresa interés en capacitar a todos los empleados en seguridad organizacional, física y tecnológica, reconociendo la necesidad urgente de implementar controles adecuados y desarrollar una cultura de seguridad que han descuidado desde el inicio de la empresa hace seis años.

A continuación, con los datos obtenidos de dicha entrevista, generamos una nube de palabras:



Fuente: Elaboración propia

PROPUESTA DE PLAN DE ACCIÓN

Teniendo en cuenta la información recolectada de la empresa, se propone un plan de acción implementando métodos simples ajustados a las necesidades de la empresa. También, recomendaremos a la empresa contratar a una persona que se encargue de la seguridad de la información (TI). En todo caso, hasta que la contratación se concrete sugerimos a la empresa ir

avanzando con las soluciones de algunas problemáticas eligiendo como responsables a gerentes de otras áreas (como, por ejemplo, recursos humanos).

A continuación, se presenta el siguiente plan de acción enumerado en pasos:

1. Capacitación Básica en Ciberseguridad

- **Descripción**: Realizar charlas de concientización en seguridad informática para todos los empleados, enfocadas en prácticas de ciberseguridad, uso seguro de contraseñas y reconocimiento de amenazas comunes, como correos de phishing.
- **Responsable**: Encargado de Recursos Humanos, con apoyo del dueño de la empresa.
- **Recursos Necesarios**: Presentación en PowerPoint o PDF, videos introductorios gratuitos en ciberseguridad (disponibles en distintas plataformas).
- **Plazo de Implementación**: Dentro del primer mes, con sesiones de 1 hora semanales durante 4 semanas.
- **Indicadores de Éxito**: Asistencia del 100% de los empleados a las charlas y una encuesta de retroalimentación al final de cada sesión para evaluar la comprensión de los conceptos básicos.

2. Instalación de Antivirus Gratuito

- **Descripción**: Implementar un antivirus gratuito en todos los equipos de la empresa para proteger de amenazas básicas.
- **Responsable**: Encargado de Tecnología (o el empleado más experimentado en sistemas, en caso de no haber un departamento específico de IT).

- **Recursos Necesarios**: Antivirus gratuitos, como Avast Free Antivirus o Bitdefender Free.
- **Plazo de Implementación**: Durante la primera semana.
- **Indicadores de Éxito**: Todos los dispositivos deben contar con antivirus instalado y realizar análisis automáticos al menos una vez por semana.

3. Fortalecimiento de Contraseñas en Activos Críticos

- **Descripción**: Implementar una política de contraseñas seguras, especialmente para el acceso a sistemas bancarios y archivos críticos de la empresa.
  - **Requisitos de contraseña**: Mínimo de 12 caracteres, con una combinación de letras mayúsculas, minúsculas, números y símbolos.
  - **Revisión de Acceso**: Revisión mensual de quienes tienen acceso a contraseñas de activos críticos.
- **Responsable**: Encargado de Recursos Humanos y el dueño de la empresa.
- **Recursos Necesarios**: Tutoriales sobre la creación de contraseñas seguras y el uso de gestores de contraseñas gratuitos (por ejemplo, Bitwarden).
- **Plazo de Implementación**: Durante la primera semana.
- **Indicadores de Éxito**: Cambio de todas las contraseñas críticas en el plazo estipulado y un control mensual de acceso autorizado.

4. Controles de Acceso y Gestión de Usuarios

- **Descripción**: Limitar el número de personas con acceso a información sensible, como cuentas bancarias o documentos confidenciales, y establecer un proceso formal para la creación y eliminación de usuarios en los sistemas de la empresa.

- **Asignación de Roles**: Asignar permisos específicos según el rol de cada empleado.
- **Control de Baja de Accesos**: Implementar un procedimiento de baja de accesos cuando un empleado se desvincule de la empresa.
- **Responsable**: Encargado de Recursos Humanos.
- **Recursos Necesarios**: Documento con las políticas de acceso y planilla para registro de altas y bajas de usuarios.
- **Plazo de Implementación**: Dentro del primer mes.
- **Indicadores de Éxito**: Registro actualizado de accesos activos y eliminación de accesos a los sistemas cuando un empleado es dado de baja.

5. Implementación de Copias de Seguridad (Backups)

- **Descripción**: Establecer un protocolo de copias de seguridad para archivos críticos. Realizar un respaldo de datos semanalmente en dispositivos externos o en la nube gratuita (Google Drive o servicios similares).
- **Responsable**: Encargado de Tecnología o persona designada.
- **Recursos Necesarios**: Disco duro externo o cuenta en un servicio de nube gratuita.
- **Plazo de Implementación**: Segunda semana.
- **Indicadores de Éxito**: Realización de una copia de seguridad semanal y la verificación de que el respaldo se mantiene accesible y actualizado.

6. Política de Protección de Datos

- **Descripción:** Desarrollar una política clara sobre la protección de datos que defina cómo se recopilan, almacenan y usan los datos sensibles. La política debe incluir prácticas sobre:
  - Acceso controlado: Solo los empleados autorizados deben acceder a dichos datos.
  - Uso restringido: Los datos sólo deben usarse para fines específicos y relacionados con la operación.
- **Responsable:** Encargado de Recursos Humanos y asesoría legal, si está disponible.
- **Recursos Necesarios**: Documento en Word que explique la política, accesible a todos los empleados.
- **Plazo de Implementación:** Primera semana.
- **Indicadores de Éxito:** Política documentada y comunicada a todos los empleados, con una revisión anual para actualizarla según la normativa vigente.

7. Evaluación Mensual de Seguridad

- **Descripción**: Realizar evaluaciones mensuales para revisar la efectividad de las medidas implementadas, incluyendo el uso de antivirus, el estado de las contraseñas, los controles de acceso y la realización de copias de seguridad.
- **Responsable**: Encargado de Recursos Humanos y dueño de la empresa.
- **Recursos Necesarios**: Lista de verificación de cumplimiento.
- **Plazo de Implementación**: Inicio de la evaluación al final del primer mes y luego mensualmente.

- **Indicadores de Éxito**: Completitud de todas las medidas de seguridad y ajustes necesarios según resultados de cada evaluación mensual.

SEGUIMIENTO Y EVALUACIÓN DE RESULTADOS

Una vez establecido el plan, para llevar un seguimiento y un control de este, utilizaran los siguientes indicadores de seguimiento y evaluación:

- **Reducción de Incidentes**: Disminución de incidentes de seguridad reportados, como acceso no autorizado o pérdida de datos.
- **Conformidad del Personal**: Nivel de cumplimiento del personal con la política de contraseñas y el protocolo de copias de seguridad.
- **Resultados de Evaluación Mensual**: Cumplimiento total de cada punto de la lista de verificación en las evaluaciones mensuales.

Este plan de implementación permite a la Pyme fortalecer su seguridad informática de manera estructurada y con bajo presupuesto, adaptándose a los recursos y conocimientos disponibles.

RESULTADOS

ANALISIS Y VALORACION DE LOS RESULTADOS OBTENIDOS

1. **Capacitación en Ciberseguridad**: El resultado de esta intervención reflejaría una comprensión mejorada de las prácticas de seguridad, demostrada por una mayor sensibilización

hacia el uso de contraseñas seguras y la identificación de amenazas como correos de phishing. Esto se validará a través de encuestas que miden la comprensión de los conceptos.

2. **Instalación de Antivirus**: Implementar antivirus debería brindar una defensa ante amenazas básicas. Si todos los dispositivos cuentan con antivirus actualizado y análisis semanales, se prevé una disminución de incidentes causados por malware, y la protección de la infraestructura de TI de la empresa se vería mejorada, reduciendo el tiempo de inactividad y las interrupciones.

3. **Fortalecimiento de contraseñas**: La adopción de contraseñas seguras y su gestión restringida a personal autorizado minimizaría los accesos no autorizados. El indicador de éxito es el cambio efectivo de contraseñas de activos críticos y el cumplimiento de revisiones mensuales.

4. **Controles de Acceso y Gestión de Usuarios**: Al implementar una gestión de accesos más estricta, se espera que la empresa reduzca riesgos de fuga de información. Este control permitiría que cualquier baja de un empleado tenga como resultado la desactivación automática de accesos.

5. **Implementación de Copias de Seguridad**: Con copias de seguridad semanales, la empresa debería estar preparada para restaurar datos rápidamente en caso de incidentes. Este protocolo puede evitar pérdidas de información crítica. El indicador de éxito en este caso es la realización consistente de copias de seguridad. El cumplimiento de esta práctica reduciría el impacto de incidentes de pérdida de datos y mantendría la operatividad de la empresa ante fallas del sistema.

6. **Política de Protección de Datos**: Implementar esta política permitiría un manejo adecuado de datos sensibles. La empresa lograría una mejor gestión de la información personal

y reduciría riesgos legales. El éxito se medirá a través del nivel de cumplimiento de la política por parte del personal y revisiones anuales.

7. **Evaluación Mensual de Seguridad**: Las evaluaciones mensuales deberían servir para identificar debilidades y optimizar continuamente las prácticas de seguridad. Si el cumplimiento es constante, el indicador de éxito mostrará mejoras en la infraestructura de seguridad cada mes.

CONCLUSIONES

El plan de seguridad informática para la empresa planteada demuestra cómo una estrategia de bajo costo, centrada en la concientización, podría fortalecer significativamente la protección de datos y reducir vulnerabilidades comunes. Las recomendaciones abarcan prácticas clave, como el control de acceso, el uso de contraseñas seguras y la implementación de copias de seguridad periódicas, que no sólo reducirían el riesgo de incidentes, sino que también fomentaría una cultura de ciberseguridad en la organización, aumentando su resiliencia operativa y su reputación en el mercado.

A pesar de los beneficios proyectados, el enfoque teórico presenta ciertas limitaciones. La dependencia de herramientas gratuitas y la falta de personal especializado en TI en pymes podría dificultar la sostenibilidad de estas medidas frente a amenazas avanzadas. Además, la capacitación y concientización, aunque necesarias, no garantizan la adopción constante de estas prácticas por parte de todos los empleados sin un refuerzo adecuado.

Para optimizar la efectividad de este plan, se recomienda designar un responsable de seguridad informática dentro de la empresa. Esta persona se encargaría de supervisar la implementación y el cumplimiento de las políticas de seguridad, y de realizar adaptaciones

según la evolución de las amenazas. También se sugiere considerar inversiones en herramientas de seguridad avanzadas y establecer capacitaciones continuas para mantener actualizado al personal. Finalmente, reforzar las políticas de acceso permitiría que solo el personal autorizado maneje información sensible.

Futuros estudios podrían profundizar en el uso de servicios de ciberseguridad en la nube como una alternativa accesible, así como investigar cómo la cultura organizacional influye en la efectividad de las políticas de seguridad y explorar estrategias de incentivos para incrementar el compromiso de los empleados con la ciberseguridad.

ANEXO

Preguntas de la entrevista:

1. ¿Tienen algún conocimiento sobre la Seguridad de la información y su importancia?

2. ¿Qué sistema de información utilizan?

3. ¿Tienen identificado cuáles son sus activos más críticos?

4. ¿De qué manera protegen estos activos?

5. ¿Es estrictamente necesario para su labor, que esas 4 personas tengan la contraseña de los bancos?

6. ¿Tienen un plan de contingencia en caso que ocurra algún incidente?

7. En caso que un empleado renuncie o sea despedido. ¿La baja de accesos al sistema es automática?

8. ¿Cuentan con firewalls o antivirus? ¿Realizan copias de seguridad?

9. ¿Te gustaría que todos en la empresa, incluyéndote, se capaciten en controles organizacionales, físicos y tecnológicos?

REFERENCIAS BIBLIOGRÁFICAS

- Baca Urbina, G. (2016). *Introducción a la Seguridad Informática*. Patria.
- INCIBE. *Gestión de Riesgos: Una guía de aproximación para el empresario*. Instituto Nacional de Ciberseguridad.
- INCIBE. *Respuesta a incidentes: Políticas de seguridad para la Pyme*. Instituto Nacional de Ciberseguridad.
- Laudon & Laudon. (2013). *Sistemas de Información Gerencial*. Pearson.