Las Políticas de seguridad e integridad de la administración de TI en una empresa que fabrica bebidas gaseosas

¿Son adecuadas para que el personal del departamento de producción tenga el conocimiento necesario y actúe de forma responsable para asegurar la integridad de la información almacenada generada y transmitida?

Asignatura: Tecnología de la Información en una Sociedad Global

Conteo de palabras: 3986

"*Confirmo que soy el autor de este trabajo y que no he recibido más ayuda que la permitida por el Bachillerato Internacional. He citado debidamente las palabras, ideas, o gráficos de otra persona que se hayan expresados estos de forma escrita, oral o visual***"**

Índice

Introducción

Hoy en día, la mayor parte de información dentro de una empresa se maneja mediante sistemas de TI que facilitan el procesamiento y almacenamiento de datos. El uso de tecnologías brinda muchas ventajas al trabajador de la empresa al momento de administrar su información, realizando sus actividades con más eficiencia. Sin embargo, cada día surgen nuevas amenazas de TI que puedan vulnerar esta información a través de ataques cibernéticos como virus o robos. Por lo que es importante que las empresas garanticen la seguridad e integridad de su información a través de políticas de TI, ya que podría ser muy importante para la toma de decisiones en un futuro.

Usualmente, las empresas cuentan con un departamento de TI que se encarga de desarrollar las políticas de TI que rigen el acceso y utilización de la información, hardware, software y redes. El objetivo de las políticas es establecer los lineamientos a seguir para la seguridad y protección de los equipos, información, sistemas y servicios para los trabajadores de la organización. (www.seguro.de.com, 2019) Las políticas de TI son importantes dentro de la organización para evitar cualquier tipo de pérdida, robo o mal uso de la información que perjudicaría crucialmente a la empresa. La información constituye uno de los recursos principales para la organización, siendo esencial para la gestión de proyectos, el planteamiento de objetivos y la toma de decisiones dentro de los procesos de la empresa.

Por lo tanto, el propósito de este trabajo es analizar cómo una empresa que fabrica bebidas realiza el cumplimiento y seguimiento de las políticas que van dirigidas a la protección y seguridad de la información dentro del área de producción. Está área maneja información muy importante como procesos de producción, gestión de proyectos calidad del producto, eficiencia en las líneas de producción, inventario y costos. Por lo que es fundamental tener medidas para la seguridad e integridad de los datos. El área de producción cuenta con cinco líneas de producción principales, en donde participan trabajadores, jefes de área, gerentes y directores, los cuales hacen uso de esta información cotidianamente. Una cualidad muy importante de esta empresa es la calidad del producto, en donde hay procesos definidos en el área de producción para mantener

esta calidad. Por lo que es importante establecer medidas que aseguren esta información. El departamento de TI de la empresa es el responsable de regular el cumplimiento de las políticas de TI dentro del área de producción y difundir la importancia para la protección e integridad de los datos que se manejan. Se deben promover estas políticas, a través de comunicados o carpetas, a todo trabajador que labore dentro de la empresa.

Además, es importante que toda política de TI se actualice constantemente, tomando nuevos riesgos que podrían perjudicar la seguridad de los datos que se almacenan en el sistema de TI. Las políticas de TI proporcionan las bases para delimitar las responsabilidades el uso de la tecnología que involucren datos importantes para la empresa. Por lo tanto, la pregunta de investigación planteada es: **¿Son adecuadas para que el personal del departamento de producción tenga el conocimiento necesario y actúe de forma responsable para asegurar la integridad de la información almacenada generada y transmitida?**

El objetivo de este trabajo es conocer el impacto que tienen las políticas de TI tanto en la información como en los trabajadores de la empresa, y como interactúan trabajadores con las normas, verificando si son conscientes de la importancia de estas políticas. También se analizará que procedimientos que realiza el departamento de TI para regular el cumplimiento de las políticas de TI dentro de la empresa. Se eligió esta empresa que fabrica bebidas, ya que su información es sumamente confidencial e importante para ser líder en el mercado.

Para desarrollar esta investigación, se analizaron los recursos que utilizan otras empresas para desarrollar y mantener sus políticas de seguridad e integridad, lo cual constituye la base para el análisis, discusión y evaluación de las fuentes primarias obtenidas dentro de la empresa. Luego, se compararon con las fuentes primarias obtenidas, es decir las políticas de TI que hacen referencia a la seguridad e integridad de la información de la empresa que fabrica bebidas. También se realizaron entrevistas y encuestas a varios trabajadores del área de producción para analizar la importancia que le dan a estas políticas y como contribuyen en la seguridad, confiabilidad e integridad de la información procesada y almacenada dentro del sistema que manejan. Por otra

parte, se entrevistó a personal del departamento de TI para conocer cómo regulan el cumplimiento de las políticas, y que consecuencias hay en caso de que un usuario viole las normas. Esto ayudará a conocer el impacto que tienen estas políticas en los trabajadores y su información para comprobar si son lo suficientemente aceptables para la integridad y seguridad de los datos que se manejan en el área de producción.

Como aseguran las empresas la seguridad e integridad con la ayuda de las políticas

Al investigar políticas de TI de varias empresas que hacen referencia la seguridad e integridad de la información, se pudo observar que los principales aspectos que abarcan son los siguientes:

- Privacidad y confidencialidad de la información: Comprende que la información únicamente será compartida a personal autorizado por la empresa, y que toda información almacenada es propiedad intelectual de la organización. El intercambio de información a personas que no forman parte de la empresa queda totalmente prohibido, ya que se pone en riesgo la privacidad de la información. (Manual de Políticas de Seguridad Informática, Cámara de Comercio Aburrá, 2016)
- Almacenamiento correcto de datos: Asegura que la información se almacene de manera correcta, para que los datos sean exactos y confiables. Estas normas comprenden todo tipo de respaldo de datos y planes de contingencia. (Política de Tecnologías de Información y Comunicación TIC, Celsia, 2013)
- Componentes de TI autorizados: La instalación y uso de componentes de TI como softwares, servicios o programas están bajo la autorización y supervisión del departamento de TI de la empresa, los cuales deben contar con una licencia establecida por la organización.
- Defensa contra ataques informáticos: Son todas aquellas medidas que buscan la protección de los datos ante posibles virus informáticos que podrían eliminar información fundamental de la empresa a través de internet y redes. (Manual de Políticas de Seguridad Informática, Contraluría Municipal de Tuluá, 2016)
- Autenticidad del usuario: comprende todo tipo de cuentas y contraseñas asignadas al usuario para establecer que información tiene autorizada y evitar la manipulación de datos por personal no autorizado.
- Protección física de los equipos: Son las medidas necesarias para proteger los equipos de cómputo que contienen información crucial para la empresa,

asegurando cualquier tipo de contacto de personas no autorizadas a la información.

Impactos en el empleo de las políticas de seguridad e integridad sobre la información

En primer lugar, todo tipo de información compartida, ya sea en correo electrónico o físicamente, está únicamente permitida para personal autorizado de la empresa manteniendo la confidencialidad y privacidad de la información. Es muy importante que la transmisión de datos del área de producción se maneje de forma confidencial ya que, si una persona no autorizada la obtiene, podría perjudicar las operaciones de la empresa. En el área de producción muchas veces se trabajan con datos muy confidenciales como productos nuevos, estrategias de mejora o proyectos a implementar. Estos datos podrían ser cruciales para la competencia que se dedica a la industria de bebidas, por lo que se debe mantener confidencial entre personal autorizado como jefes de área o gerentes. Además, todo tipo de datos como costos o transacciones que maneja el área de calidad en producción debe ser controlado únicamente por jefaturas y gerencias, y no debe ser difundido a cualquier trabajador, porque esa información se podría filtrar fuera de la empresa.

Para conocer de mejor forma que importancia tienen las políticas para los trabajadores, se realizaron entrevistas a las siguientes personas del área de producción:

- Programador de mantenimiento
- Jefe de Calidad
- Supervisora de Producción

Los tres trabajadores demostraron conocer las políticas y su importancia para mantener la confidencialidad y privacidad de los datos. El programador de mantenimiento menciono que maneja muchos proyectos de instalación y mantenimiento en las líneas de producción, por lo que esa información no se puede difundir hasta que se tenga todo preparado para implementarlo. (Menéndez, 2019) Además, últimamente se han querido implementar nuevos productos al mercado, lo cual esta información resulta ser muy

confidencial. La Jefe de Mantenimiento menciona que la información que maneja es muy delicada ya que controla las autorizaciones de dinero y compra dentro del área de producción. (Ruth, 2019) Esos datos no se comparten a ninguna persona fuera de la empresa, y únicamente es manipulada por gerencia. Luego la Supervisora de Producción expreso que toda la información del proceso de la producción es privada para la empresa, ya que es un proceso único que diferencia su producto de los demás. (Castañeda, 2019) Por lo que todo trabajador tiene establecido no proporcionar esa información a gente exterior de la empresa.

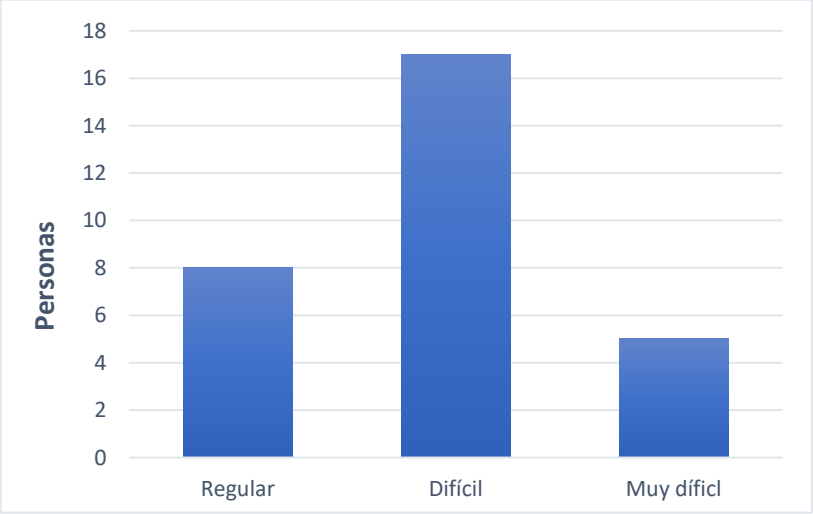
Continuando con el tema, todo componente de TI debe estar autorizado por el departamento de TI de la empresa, ya que la instalación de cualquier programa o servicio no licenciado por la organización podría ser un riesgo para la información almacenada y podría generar cambios dentro del sistema de TI. El departamento de TI, para regular esto, cuenta con una plataforma para la autorización de cualquier equipo físico o software donde la persona solicita y justifica el uso de una nueva herramienta. Es muy importante que el software que procesa los datos e información de las líneas de producción sea confiable para que ningún dato se pierda y todo se almacene de manera correcta. En las entrevistas, los trabajadores consideran que la información y los datos se están almacenando de manera correcta, ya que el sistema de TI que utilizan es muy confiable y nunca les ha generado problemas técnicos.

Por otro lado, cada cierto tiempo se actualizan plataformas en la cual se elimina alguna información que no es relevante para la compañía. Por lo que todo tipo de retención o eliminación de datos debe solicitarse y ejecutarse por el departamento de TI y el área a que corresponde la información. Es importante tomar esto en cuenta ya que una persona no autorizada podría ejecutar estas acciones y eliminar información importante por equivocación. Además, cuando un personal de la empresa es despedido o trasladado, el departamento de TI solicita que la persona entregue su usuario y contraseña, para que ningún tipo de información salga de la compañía y que el acceso a los datos sea restringido a personal que no labore dentro de la empresa.

Impactos en el empleo de las políticas de seguridad sobre los trabajadores

En primer lugar, cada trabajador debe tener un usuario y una contraseña específica, el cual se responsabiliza por el uso correcto de la información y el resguardo de las contraseñas para acceder al sistema de TI. En la entrevista realizada El Jefe de informática mencionó que: “Es importante que cada trabajador tenga un usuario y contraseña establecida, para garantizar que no tendrá acceso a transacciones que no competen a sus atribuciones.” (Morales, 2019) Los usuarios y contraseñas ayudan a que cualquier trabajador no pueda manipular o alterar los datos almacenados en el sistema, lo cual contribuye a mantener la integridad de los datos

Además, el usuario debe emplear una contraseña altamente segura para que personal no autorizado pueda acceder a su equipo y logre manipular datos importantes aportando a la exactitud de la información. Mensualmente, el mismo sistema pide al usuario cambiar la contraseña del sistema, en caso de que alguien descubra la contraseña y piense utilizarla a largo plazo. Para analizar la importancia que le dan los trabajadores de producción a las contraseñas seguras, se realizó una encuesta del nivel de dificultad que consideran que tiene su contraseña:



Gráfica 1: Cantidad de personas según la dificultad de la contraseña, encuesta agosto 2019

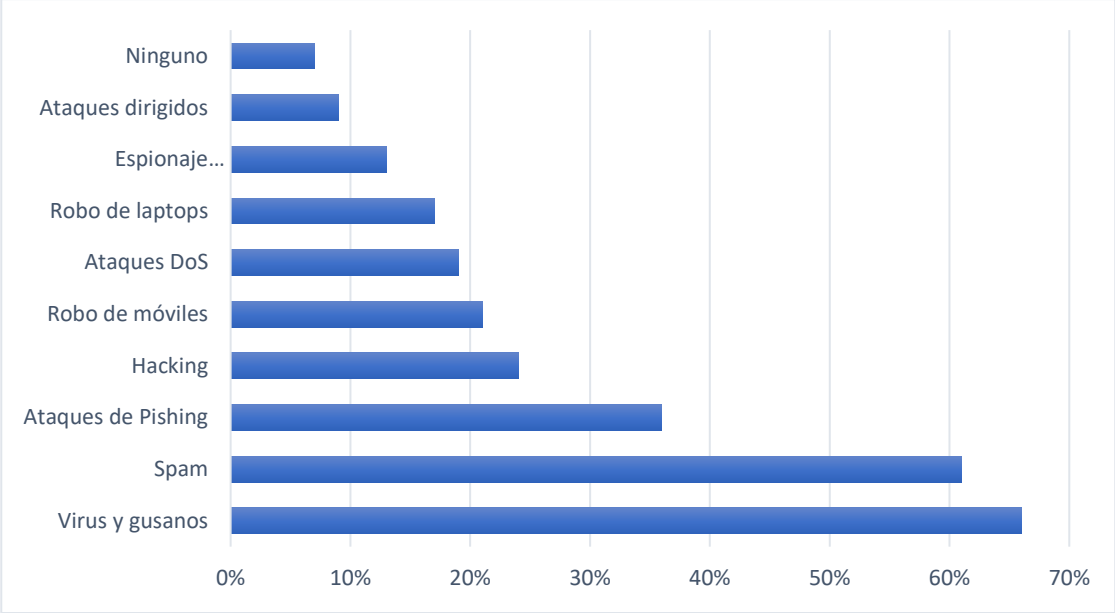
Tabla 1

Dificultad	Personas
Regular	8
Difícil	17
Muy difícil	5

Se puede observar en la gráfica 1 que la mayor cantidad de trabajadores consideran que su contraseña es adecuadamente difícil. Sin embargo, ellos mencionan en las entrevistas

que, si utilizan una contraseña demasiado complicada podrían llegar a olvidarla, ya que constantemente la actualizan. Mientras que otras personas no tienen problema con eso, y prefieren utilizar una contraseña altamente difícil.

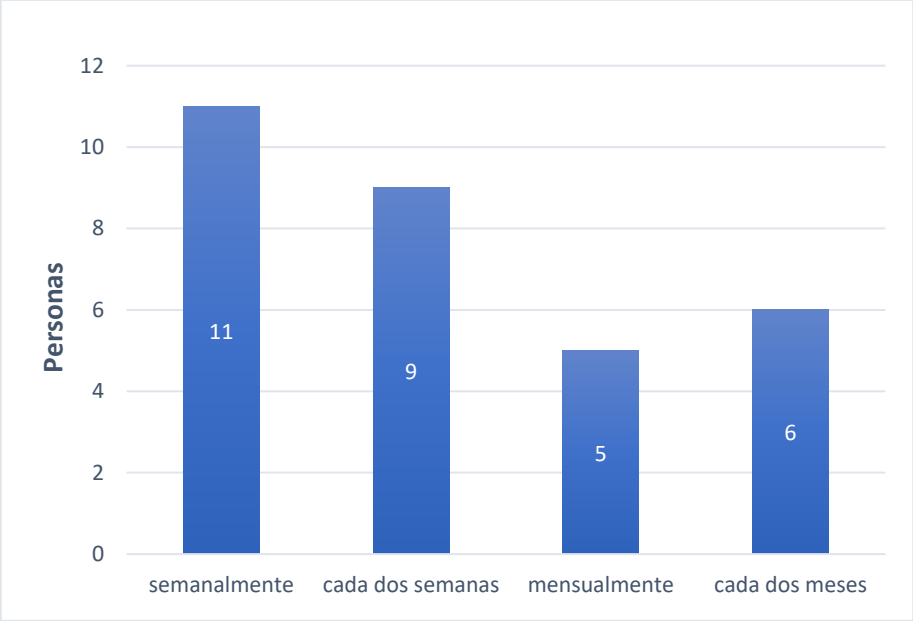
Por otro lado, es importante que los usuarios no visiten páginas con contenido ilícito, ya que podrían ser un riesgo en cuanto a ataques informáticos. Cualquier tipo de malware podría manipular o borrar datos del equipo de cómputo, por lo que estos equipos cuentan con un antivirus instalado que se actualiza periódicamente para proteger la información de la empresa. Un estudio hecho por Kaspersky en 2013 se observó que el 91% de las empresas han sido víctimas de ataques cibernéticos (Kaspersky.es, 2013). En la gráfica 2 se muestra un porcentaje de los distintos ataques cibernéticos que las empresas sufren, donde gran porcentaje son virus y gusanos. Por lo que es muy importante que la empresa tome medidas con respecto al uso de redes y unidades extraíbles.



Gráfica 2: Porcentaje de empresas con ataques cibernéticos (Kaspersky.es 2013)

En el caso de compartir información vía e-mail, el correo cuenta con una serie de especificaciones donde se informa que la divulgación, retransmisión, distribución, copia o cualquier uso de la información transmitida está totalmente prohibida. Esto ayuda a hacer conciencia el tipo de información que comparte el trabajador a través de su e-mail cotidianamente transmitiendo a cada usuario la importancia de la privacidad de los datos para la empresa.

Luego, el departamento de TI otorga a cada trabajador un disco duro para que respalde la información de su equipo de cómputo, garantizando que los datos estén almacenados de forma segura. Con un respaldo frecuente, la pérdida de información no podrá afectar al trabajador, por lo que las políticas establecen que el respaldo debe realizarse al menos dos meses. Cada trabajador dentro del área de producción se responsabiliza por respaldar su información, y asumir las consecuencias en caso de que se pierdan esos datos. Se observó que la mayor parte de los trabajadores respaldan su información semanalmente para evitar cualquier perdida de sus datos. En la siguiente gráfica se observa la cantidad de personas que respaldan su información según la frecuencia con la que lo realizan:



Gráfica 3: Cantidad de personas según la frecuencia de los respaldos, encuesta agosto 2019

Tabla 2

Frecuencia	Personas
semanalmente	11
cada dos semanas	9
mensualmente	5
cada dos meses	6

Por otro lado, es muy importante la protección física de los equipos de cómputo ya que contienen información crucial de la empresa. El resguardo físico de los equipos asegura cualquier tipo de contacto de personas no a autorizadas a la información. Según las entrevistas hechas, todos los usuarios cuentan con cartas de responsabilidad por el resguardo físico de los equipos de TI asignados en donde cualquier daño o perdida que le ocurra al equipo cae sobre la responsabilidad del trabajador. Por lo tanto, los equipos de Ti deben estar vigilados por el usuario en todo momento.

Análisis de como las políticas de la empresa son lo suficientemente aceptables

Las políticas de TI de la empresa tienen establecido que la información y datos contenidos dentro del sistema de TI son considerados como propiedad intelectual dentro del área de producción. (FEMSA, Manual de Políticas Corporativas, 2017) Esto hace que quede totalmente prohibido compartir datos privados a personas externas de la empresa, y que no se realicen copias de datos confidenciales. Todo tipo de información de planificación de proyectos, inventario y procesos de producción son fundamentales para mantener la esencia del producto y de la empresa, contribuyendo altamente a la protección de la información que maneja la organización.

Estas políticas son totalmente efectivas ya que todo usuario debe considerar la criticidad y sensibilidad de la información al momento de ser almacenada y procesada por los sistemas y equipos de TI. Las políticas de TI buscan proteger la integridad de la información para que los datos sean exactos y tengan una alta efectividad al momento de trabajar. Toda retención y destrucción de datos almacenados deben solicitarse y ejecutarse cuando sean requeridos por el dueño asociado a la información, evitando cualquier perdida de información importante. Al igual que las demás empresas, los trabajadores deben realizar el respaldo de la información periódicamente en medios y equipos que sean propiedad de la empresa.

Luego, la empresa cuenta con una serie de políticas para el uso de cuentas y contraseñas en cualquier equipo o servicio de TI para poder autenticar a la persona que desee acceder a la información. (FEMSA, Política de Contraseñas y Cuentas de Acceso, 2014) En primer lugar, menciona que a todo personal autorizado se le debe asignar su respectiva cuenta y contraseña, asegurando que no tendrá acceso a funciones que no correspondan a sus atribuciones. Las contraseñas deben obtener por lo menos ocho caracteres en los cuales se deben incluir: al menos una letra mayúscula, una minúscula, un dígito y un carácter especial. Esto asegura que las contraseñas sean altamente seguras y la clave para el acceso a la información sea imposible de descifrar. Además, Es importante que las políticas establezcan que el trabajador debe actualizar su contraseña al menos mensualmente para aumentar la seguridad en caso de que alguien

no autorizado haya descifrado la contraseña de algún usuario y desee manipular la información de forma maliciosa.

En caso de que la contraseña se ingrese incorrectamente cinco veces seguidas, la cuenta se bloquea automáticamente por un periodo de seis horas. A través de este procedimiento se verifica si es el usuario autorizado quien desea acceder a la información o es un intruso. Sin embargo, puede que el usuario haya olvidado su contraseña, por lo que debe ir al departamento de TI para solicitar un desbloqueo autorizado. Se observa a comparación de otras empresas que esta serie de políticas toman en cuenta todo tipo de circunstancias con respecto al uso de contraseñas y cuentas para proteger la información almacenada en el sistema frente a personal no autorizado.

Por otra parte, las políticas de TI establecen que las unidades de negocio deben contar con cartas de responsabilidad por el resguardo físico de los componentes de T.I. asignados a los usuarios, por lo que obliga a mantener al usuario más atento a su equipo de cómputo en todo momento. Para regular el cumplimiento de las políticas que se refieren a la protección del resguardo físico, el departamento de TI tiene establecido a un personal de seguridad que verifica cotidianamente en las oficinas que todo equipo de cómputo esté debidamente resguardado. Las computadoras que estén en un escritorio en el cual no se encuentre el usuario son reportados a gerencia y se llevan al departamento de TI. Esto asegura que cualquier persona que entre a las oficinas pueda acceder a información confidencial a través del equipo de cómputo y pueda manipularla de forma maliciosa.

Las normas que establecen los lineamientos para uso de internet y redes con que cuenta la empresa son esenciales para evitar todo tipo de virus y ataques informáticos que ponen en riesgo la seguridad de los datos. (FEMSA, Políticas de Correo Electrónico, Redes e Internet, 2014) Por esta razón el servidor central cuenta con un firewall para bloquear el acceso no autorizado, filtrando el tráfico de datos a través de la red protegiendo la información de la empresa que está almacenada. Las políticas que se incluyen en cada correo electrónico logran que cada trabajador sea consciente que tipo de información comparten en las redes, y que procedimientos son los adecuados para evitar un ataque cibernético.

Conclusiones

Se puedo observar a lo largo de la investigación que las políticas de TI son totalmente adecuadas para que el personal del departamento de producción actúe de forma responsable asegurando la integridad de la información almacenada y procesada de la empresa. Comparadas con políticas de otras empresas se puede decir que abarcan los principales aspectos que aseguran la protección y exactitud de los datos almacenados y procesados. Esto lo hace tomando en cuenta el uso de redes, usuarios y contraseñas, recursos compartidos y equipos de cómputo, que son los principales recursos que interactúan con la información de la empresa

Luego a través de las entrevistas se demuestra que los usuarios conocen las políticas de TI que regulan la seguridad e integridad de los datos del área de producción, y son conscientes de su gran importancia para mantener resguardada y confidencial la información. Por esta razón se pudo observar que las políticas de TI tienen un gran impacto para para los trabajadores y la información de la empresa. Todo trabajador que se le haya asignado un equipo de cómputo debe hacerse responsable de resguardarlo correctamente en todo momento. La confidencialidad de la información es sumamente importante para la empresa, que el trabajador no debe compartir carpetas a gente externa de la empresa, y constantemente debe hacer un cambio de contraseña que cumpla los requisitos dados. Da esta manera, el trabajador contribuye a proteger la integridad de la información. Luego, con respecto a la información, las políticas tienen establecidos los lineamientos para almacenarla de forma correcta, haciendo respaldos periódicamente que aseguren los datos en caso perdidas o robos.

Se observó que el departamento de TI es el principal responsable de dar a conocer estas políticas a los trabajadores y regular su cumplimiento cotidianamente, ya que una falta a estas políticas podría llegar a vulnerar la información y la vez perjudicar a la empresa. El departamento de TI regula el cumplimiento de sus políticas asignando a cada trabajador un perfil y una contraseña garantizando que no tendrá acceso a información que no correspondan a sus atribuciones. Constantemente el departamento de TI realiza auditorías y revisiones físicas a sus trabajadores para verificar la información almacenada en el equipo y que no posee ningún tipo de programa no autorizado. Todo

el registro de las acciones que realizan los usuarios queda en su equipo de cómputo. Por lo que cualquier acción no autorizada es reportada a gerencia. El departamento de TI también se preocupa por actualizar las políticas anualmente, dándolas a conocer a través de comunicados y correos electrónicos. Por esta razón los usuarios también resultan demostrar un comportamiento responsable ante todo tipo de información que almacenan y transmiten, teniendo en cuenta la importancia de las políticas para la seguridad e integridad de los datos.

Las políticas de TI juegan un importante papel en el área de producción de FEMSA, ya que los datos que se manejan como proyectos, índices de eficiencia, productos nuevos y sistema de calidad, son confidenciales y fundamentales para la toma de decisiones dentro de la empresa. Esta información que se maneja es sumamente importante para que la empresa siga siendo líder en el mercado y producción de bebidas a nivel mundial. Cualquier robo de datos e información podría afectarlos en sus procesos únicos de producción, ya que la fabricación de sus productos son clave de su esencia. Por eso es importante que toda instalación de software, servicios o almacenamiento de datos sea autorizada por el departamento de T.I.

A través de las encuestas realizadas se observa que los trabajadores le dan importancia al resguardo y uso de contraseñas del sistema de TI, el cual son conscientes que los datos se están almacenando de manera correcta. También se observa que los trabajadores se preocupan por respaldar su información con una frecuencia aceptable, para garantizar que los datos importantes no se pierdan. Actualmente, gran porcentaje de las empresas son víctimas de ataques informáticos los cuales son un riesgo para la integridad de los datos. Las políticas que tiene la empresa ayudan a establecer lineamientos que eviten cualquier tipo de ataque a los datos. Es importante que todos los equipos de cómputo cuenten con un antivirus ya que los virus podrían eliminar información fundamental que sea base para la toma de decisiones en el futuro, y control del departamento de producción.

Bibliografía

Castañeda, V. (29 de agosto de 2019). Importancia de las Políticas de TI. *Entrevistas a Trabajadores de Manufactura*, 19. (C. Catú, Entrevistador) Guatemala, Guatemala, Guatemala.

FEMSA, C.-C. (2014). *Política de Contraseñas y Cuentas de Acceso.* Guatemala.

FEMSA, C.-C. (2014). *Políticas de Correo Electrónico, Redes e Internet.* Guatemala.

FEMSA, C.-C. (2017). *Manual de Políticas Corporativas.* Guatemala.

Kaspersky.es. (2013). Recuperado el 15 de agosto de 2019, de Kaspersky.es: https://www.kaspersky.es/blog/las-amenazas-mas-importantes-de-2013/2008/

(2016). *Manual de Políticas de Seguridad Informática, Cámara de Comercio Aburrá.* Recuperado el 27 de agosto de 2019, de prezi.com: http://www.ccas.org.co/wp-content/uploads/2017/10/MANUAL-DE-POLITICAS-DE-SEGURIDAD-INFORMATICA-V3_2016.pdf

(2016). *Manual de Políticas de Seguridad Informática, Contraluría Municipal de Tuluá.* Tuluá. Obtenido de www.contraloriatulua.gov.co: http://www.contraloriatulua.gov.co/wp-content/uploads/2017/11/M-113-01-Manual-Pol%C3%ADticas-de-Seguridad-Inform%C3%A1tica.pdf

Menéndez, Y. (29 de agosto de 2019). Importancia de las Políticas de TI. 18. (C. Catú, Entrevistador) Guatemala, Guatemala, Guatemala.

Morales, M. (29 de agosto de 2019). Importancia de las Políticas de TI. *Entevistas a Trabajadores de Manufactura*, 21. (C. Catú, Entrevistador) Guatemala, Guatemala, Guatemala.

(2013). *Política de Tecnologías de Información y Comunicación TIC, Celsia.* Recuperado el 22 de agosto de 2019, de www.celsia.com: https://www.celsia.com/Portals/0/contenidos-celsia/nuestra-empresa/politicas-y-adhesiones/politicas/politica-tecnologias-de-informacion-y-comunicacion-tic.pdf

Ruth, M. (29 de agosto de 2019). Importancia de las Políticas de TI. 17.

www.seguro.de.com. (2019). Recuperado el 27 de julio de 2019, de www.seguro.de.com: https://www.segurode.com/noticias/ciberriesgos/valor-politicas-seguridad-informatica

Apéndice

Entrevistas a trabajadores de manufactura
Importancia de las Políticas de TI

Fecha: 29 de agosto 2019

FEMSA, área de manufactura

Ruth Medina: Jefe de Calidad

1. ¿Conoce usted las políticas de TI de la empresa? ¿Sabe porque es importante tenerlas en cuenta?

Sí, las conozco. Cuando se utiliza SAP existen políticas de tener un usuario y una contraseña que no se deben compartir con nadie. Existe también un formulario de control interno en el caso de que si yo me ausento o me voy de vacaciones puedo dar mi usuario y contraseña, pero haciendo firma de responsable de que cualquier transacción que se haga en el sistema es bajo mi código de usuario. En mi caso, la información que manejo es muy delicada ya que hay autorizaciones de dinero y compra. No se pueden instalar programas no autorizados para la empresa, si necesito un programa en específico como herramienta de trabajo tengo que hacer una solicitud dando una justificación: para qué es que voy a utilizar ese programa, porque hay programas que con solo autorización se pueden instalar

Con las políticas se tiene restricción a ciertas páginas, como redes sociales por temas de virus que pueden generar en el equipo informático. Además, con cierto periodo de tiempo se deben cambiar las contraseñas de ingreso para el correo electrónico y sistemas sensibles

2. ¿Como se considera haciendo uso responsable de las políticas de T.I.?

Me considero responsable al 100%, porque lo que es el acceso a internet me meto únicamente a las páginas que necesito. En temas de usuarios y contraseñas el mismo sistema nos pide que tengamos que estar haciendo ese refrescamiento. Con los sistemas sensibles no me ha tocado dar usuarios ni contraseñas al departamento de T.I. en casos que me ausente, cumpliendo con todas las autorizaciones.

3. ¿Ha recibido capacitación últimamente sobre el uso de TI?

No se recibe capacitación, pero constantemente nos mandan comunicados de las políticas de T.I. Cuando se ingresa a laborar en la empresa nos hacen firm.ar el código de ética, en el cual van ciertas políticas relacionadas con la parte de herramientas

Yeffri Menéndez: Programador de Mantenimiento

1. ¿Conoce las políticas de la empresa que involucran la seguridad de los datos?

Sí, esas políticas se envían por correo a todo trabajador de FEMSA anualmente. Cuando se envía un destinatario fuera de la compañía esta política dice que no debería de difundir esa información a cualquier persona. Si le llega el correo por error a alguien debería de reenviar el correo a la persona que lo envió y no difundir esa información. Las principales que conozco es no proporcionar información de la empresa que es privada.

2. ¿Cree usted que el respaldo de la información es necesario para la seguridad de los datos? ¿Qué procedimientos se realizan?

Si es muy importante. Lastimosamente ha ocurrido que a las personas se les borra lo que tienen en la computadora y se pierde por completo. Muchos lo que hacen es tener un backup de su disco duro, y respaldar la información personalmente. Yo guardo por aparte mi información en un disco duro proporcionado por la empresa.

1. ¿Considera usted que la confidencialidad de los datos es importante?

Es bastante importante porque más que todo hay muchos proyectos que se manejan en el área de manufactura y en el área que manejo muchos productos nuevos que no deben saberse solo así, sino que deben mantenerse confidencialmente por las personas responsables para luego

2. ¿Considera que cumple con las políticas de T.I. todos los días?

Sí, como estoy en el área de mantenimiento si vemos muchos temas de proyectos, por ejemplo, se va a instalar un equipo nuevo en tal lado, entonces no se puede difundir esa información hasta que ya se tenga listo todo

3. ¿Qué medidas toma la empresa para que el trabajador se haga responsable de sus equipos de cómputo?

Al momento en que se nos entregan nuestros equipos de tecnología debemos firmar un contrato en donde asegura que hemos leído las políticas, y que nos haremos responsables de la seguridad de los datos y el equipo. Es una carta de responsabilidad importante ya que uno se lleva a la casa el equipo o a la calle, y si se pierde cae en nuestra responsabilidad.

Virginia Castañeda: Supervisor de Producción

1. ¿Conoce usted las políticas de TI de la empresa? ¿Sabe porque es importante tenerlas en cuenta?

Si, es el manejo de toda la información segura, no compartir la información de la empresa, no sacar copia de los documentos confidenciales.

2. ¿Se considera responsable por el cumplimiento de las políticas de TI?

Si, por que todos tenemos acceso a la información de la parte de los procedimientos, de toda la información del proceso de la producción entonces, como supervisora de producción que soy, si tengo la responsabilidad de salvaguardar esa información

3. ¿Considera usted importante la actualización de datos en la empresa? ¿Qué procedimientos se realizan?

Nosotros manejamos casi todo eso a nivel de SAP, entonces toda la actualización es automática. Además, el sistema se actualiza constantemente, brindando mejores opciones para procesar los datos.

4. ¿Como se les hace llegar a los trabajadores las políticas de T.I. que maneja la empresa?

A través de comunicaciones, correo, carteleras que se colocan en el área de trabajo, y cuál es el manejo de la información segura.

4. ¿Como se regula la privacidad y confiabilidad de archivos compartidos dentro de la empresa?

Tenemos carpetas compartidas a nivel de una plataforma interna, es información que está compartida para varios usuarios, pero solo se tiene acceso dentro de la empresa, y es responsabilidad de cada trabajador no sacar copia de los documentos

Marvin Morales: Jefe de Bodega

1. En que han permitido mejorar la seguridad e integridad de los datos

A través de usuarios y contraseñas establecidas en todas las aplicaciones manejadas. Además, se controla la instalación de softwares y el contenido que se visualiza en las redes para evitar cualquier clase de virus.

2. ¿Qué procedimientos se realiza al momento de deshacerse de datos que ya no serán útiles?

Se hace únicamente cuando personal de la empresa es despedido. Entonces se ingresa al equipo del usuario y se extrae toda información importante. Luego el departamento de TI formatea el equipo por completo.

3. Como controlan la instalación de nuevos componentes de T.I.

En las auditorias que hacen desde México al equipo en línea con las que hacen aquí localmente, se detecta si se tiene un programa o software que no está autorizado. Eso se bloquea mandando un reporte. El reporte debe firmarse por el usuario

4. Como controlan la protección de equipos dentro de la empresa

Se tiene una persona asignada para que pase revisando las oficinas todos los días a las 12:00. Si llega a encontrar un equipo de cómputo abierto sin el usuario presente, se recoge y se reporta al departamento de TI. El usuario debe reclamar ese equipo y firmar un reporte por el fallo que hizo.

5. Considera que las políticas que están actualmente son adecuadas para la seguridad de los datos

Hoy en día considero que sí, hay mucho más control en la información. A nivel de correos, se filtran. Se bloquean correos que no tengan nada que ver con la empresa. Los dispositivos USB se prohíben también.

6. ¿Cuál ha sido la mayor dificultad que han tenido para la protección de datos?

Cuando se hacen mantenimientos, el departamento comunica fechas y horarios que van a intervenir, haciendo backup o actualizaciones. Esto lo hacen para que las personas se preparen cuando le bloqueen el acceso al sistema.

Erick Uriza: Jefe de Informática

1. ¿Qué procedimientos realiza al compartir información privada de la empresa?

El correo electrónico cuenta con políticas en caso de que alguien haya recibido el correo por equivocación. No se permite compartir información privada a gente que no sea de la empresa, ni mucho menos sacas copias.

2. ¿Como regulan la instalación de nuevos componentes de T.I.?

A través de una plataforma llamada SOLIN donde se solicita la instalación de nuevos componentes, tanto software como hardware.

3. ¿En caso de virus informáticos, que procedimientos se realizan para mantener segura la información?

Los virus son reportados al departamento, y se interviene al equipo de cómputo para verificar si toda la información se encuentra segura. Además, todos los equipos cuentan con un antivirus llamado Symantec.

4. ¿Qué medidas tienen establecidas en caso que alguien no cumpla con las políticas de T.I.?

Es reportado al departamento de TI y a gerencia, donde el usuario debe firmar de no haber cumplido con las políticas y gerencia toma medidas según el caso

5. Cada cuanto actualizan las políticas de TI

Como parte del proceso que hay de gestión, año con año se validan las políticas desde el corporativo situado en México. Además, se hacen campañas para el cumplimiento de estas políticas.

6. ¿Como regulan el resguardo de los equipos de TI?

Se pasa una revisión todos los días. Si se encuentra una laptop desplegada sin el usuario presente se reporta, y se envía a gerencia, ya que cualquiera que entre a la oficina podría tener acceso a esa información.

7. ¿Como regulan el cumplimiento de las políticas de TI?

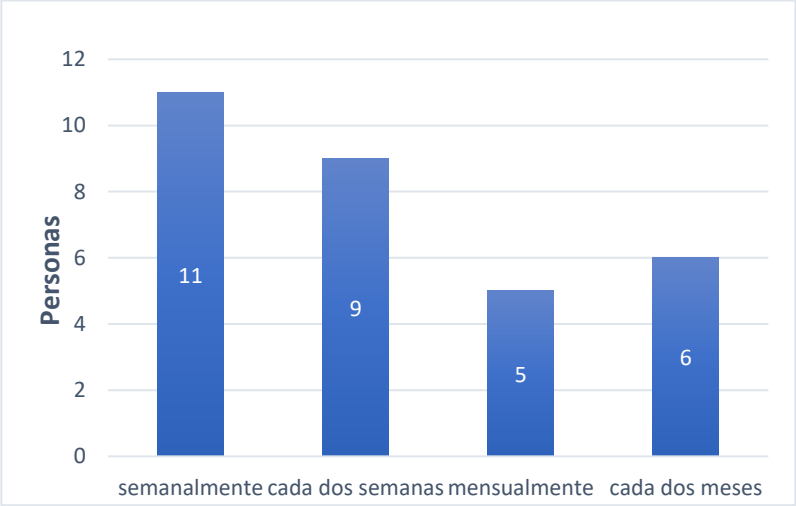
Primero que todo, es importante que cada trabajador tenga un usuario y contraseña establecida, para garantizar que no tendrá acceso a transacciones que no competen a sus atribuciones.

Mediante auditorias físicas del sistema, revisiones en línea cuando uno está conectado haciendo verificaciones de la información que se tiene almacenada. Todos los registros quedan grabados, y pueden consultarlos cualquier operación en el sistema. Además, todo equipo que no pertenezca a la empresa debe estar documentado.

Encuestas a trabajadores de FEMSA

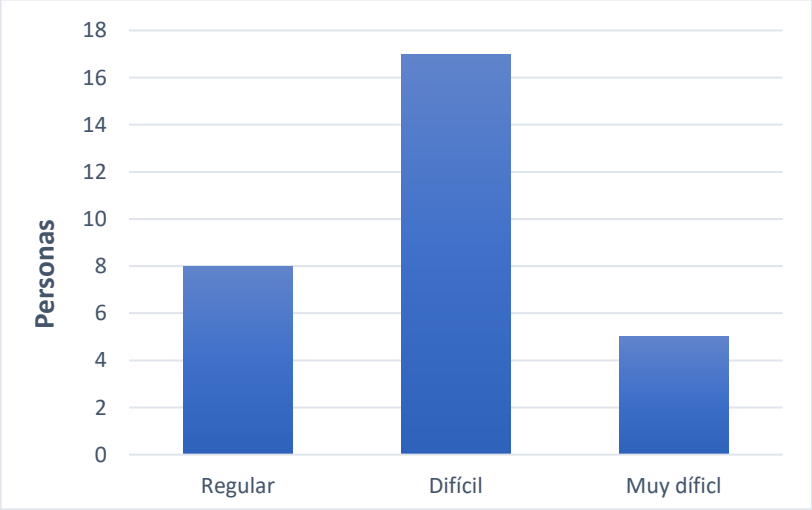
Fecha: 3 de septiembre d 2019
Lugar: FEMSA, área de manufactura

1. ¿Como considera usted la dificultad de su contraseña?



Dificultad	Personas
Regular	8
Difícil	17
Muy difícil	5

2. ¿Con que frecuencia respalda usted sus datos?



Frecuencia	Personas
semanalmente	11
cada dos semanas	9
mensualmente	5
cada dos meses	6