UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

JUNIO –SEPTIEMBRE 2020

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCION DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

PROPUESTA PARA EL CONTROL Y SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA DE VENTAS EN LÍNEA BUY NOW APLICANDO NORMA ISO 27001

EGRESADO:

GALO MIGUEL CAMPOSANO MONAR

TUTOR:

ING. IVAN RUBEN RUIZ PARRALES, MSC.

AÑO 2020

INTRODUCCION

Se procederá a desarrollar en este proyecto un estudio del control y seguridad informática de igual manera se realizara un análisis de riesgos a la empresa, la misma que efectúa sus ventas Online. Con el fin de liberar la solidez de los sistemas de información y del control, la eficacia y confianza en los programas y operaciones, en el cumplimiento de las leyes y normas aplicables.

El proyecto de implantar este procedimiento es preservar la información plena y total de los activos y pasivos en dicha empresa, con la finalidad de conseguir confidencialidad, integridad y disponibilidad de los datos, la designación de responsabilidades que debe asumir cada uno de los funcionarios de la organización, desempeñando las políticas previamente implantadas con el propósito de garantizar el pleno proceso de la actividad comercial de la empresa.

Es preciso emplear esta norma debido a que las políticas de seguridad informática existentes deben ser fortalecidas y que cada usuario de la organización se comprometa a cumplir con las mismas en sus tareas habituales, la Norma ISO 27001 se encarga de implantar estrategias y compromisos claves con el fin de proteger la información plena y total de las activos y pasivos de la organización.

Se llevará a cabo un plan de seguridad informática, donde se definen los lineamientos de la planeación, el diseño e implantación de un modelo de seguridad con el objetivo de establecer una cultura de la seguridad en la empresa. De esta manera obliga a la misma la implementación de procedimientos estandarizados de seguridad, los cuales deben estar enmarcados en el proceso que conforman dicho plan.

La línea de investigación que está regido el estudio de caso es Desarrollo de sistemas de la información, comunicación y emprendimientos empresariales y tecnológicos; y como Sublíneas Redes y tecnologías inteligentes de software y hardware.

DESARROLLO

Este compromiso se establece en las medidas de control y seguridad de la información de empresa en las ventas Online Buy Now, está ubicada en la avenida Universitaria entre la calle la tercera y cuarta transversal de la ciudad de Babahoyo, Provincia de Los Ríos, Republica del Ecuador.

Los errores que se hallan en la empresa Buy Now por ventas Online, resultan del hecho de no haber aplicado estrategias de seguridad en la información de una manera firme para una correcta operación en actividades de compra venta.

Auditoría en Seguridad Informática

Se trata de un servicio llevado a cabo por profesionales externos a una empresa y tiene la finalidad de descubrir posibles vulnerabilidades tras revisiones exhaustivas de software, redes de comunicación, servidores, estaciones de trabajo, dispositivos móviles, etc.

Auditoría Informática una serie de análisis periódicos o casuales de un sistema informático cuya finalidad es analizar y evaluar la planificación, el control, la eficacia, la seguridad, la economía y la adecuación de la infraestructura informática de la empresa. (Bracho-Ortega & Cuzme-Rodríguez, *et al*., 2017; Sánchez-Henarejos et al., 2014).

Importancia de la Auditoría Informática

Cada día cobra una mayor importancia el realizar una auditoría de Seguridad a estos componentes, para conocer exactamente las vulnerabilidades de nuestros sistemas y los riesgos a los que están expuestas las empresas, para así prevenir consecuencias indeseables.

Los sistemas informáticos se encuentran especialmente expuestos al ataque de usuarios maliciosos, hackers y otra serie de intromisiones que pueden afectar severamente, el correcto funcionamiento de los sistemas y se puede ver comprometida información sensible de los procesos de negocio soportados por estos sistemas (Soto et al., 2017).

Norma ISO 27001

Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan (Ruíz Tapia et al., 2020).

Estructura de la Norma ISO 27001

Para el cumplimiento de dicha estructura de debe llevar a cabo paso a paso cada punto (Ascanio et al., 2015).

1. Objeto y campo de aplicación
2. Referencias Normativa
3. Términos y Definiciones
4. Contexto de la Organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del Desempeño
10. Mejora

Beneficios de la Norma ISO 27001

Es certificable, la norma ISO 27001, por tener un reconocimiento difundido a cualquier empresa que tenga establecido un SGSI (Sistema de Gestión de la Seguridad de la Información)

puede solicitar una Auditoría a una entidad acreditada para obtener la legitimación del sistema ISO 27001. Es de ayuda mencionar: (Basantes, & Bahamonde, 2017).

1. Entre los beneficios de la norma, muestra que la garantía independiente de los controles internos cumple con los requisitos de Gestión Corporativa y de continuidad de la actividad comercial.
2. Facilita un adelanto profesional para cumplir las exigencias establecidas y poder expresar a los usuarios que la seguridad de su información es fundamental.
3. El resultado a las evaluaciones constantes, refuerza el conocimiento periódico en beneficio y progreso de la empresa.

Certificación:

1. **Crear los estándares de formación**

Para desarrollar y estandarizar la formación, se debe orientar mediante seminarios y talleres, para adquirir los conocimientos siendo la función el adaptar las instrucciones que se han solicitado, para ser aplicadas según la certificación y así asumir las molestias en el sistema de seguridad en cualquier organización.

2. **Selección de la norma**

Para beneficiar a la empresa se debe seleccionar la norma, para luego formalizar el requerimiento adecuado mediante la obtención y certificación.

3. **Apoyo empresarial**

El apoyo como institucion a la empresa es muy necesario, siendo tan importante la relación por conocimiento a los funcionarios, donde sus obligaciones son sustanciales para un buen desarrollo y entrega de los estándares a la organización, con ello se orientará el convenio al costo y el período que se supone serán evaluados.

4. **Valoración y Observación**

Se efectúa la valoración al procesos operacional del sistema y a la gestión de seguridad informática, por cualquier complicación se realizan las observaciones y

poder satisfacer cualquier necesidad a la información, proporcionando una evaluación justa y exclusiva para la organización empresarial.

5. Certificación al proceso informático operacional

Una vez que se concluya con la valoración, se solicitara se emita el correspondiente certificado de registro como beneficio a la certificación, este documento tiene como duración tres años, siendo el delegado de la empresa quien visite de manera constante y brinde la ayuda necesaria, garantizando el cumplimiento como requisitos a otorgar el soporte continuo a los sistemas (Melo, & Hernando, 2008).

Evidencias que muestren la evaluación mediante la Norma ISO 27001

ISO. Organización que establece las normas y las promociona.

ISO 27001. Establece los requisitos para la implementación de un SGSI.

Objetivo.- Es el resultado que se desea lograr usando los procedimientos implementados.

Plan de tratamiento de riesgos. Documentación que define qué acciones tomar para gestionar el riesgo de la seguridad de la información.

Proceso. Actividad que tiene como existencia un producto.

Riesgo. Se manifiesta cuando una amenaza explota una vulnerabilidad.

Tratamiento de riesgos. Proceso que aplica controles para mitigar el riesgo.

Vulnerabilidad. Debilidad no evidente en un activo.

1. Obtener el compromiso de la alta dirección
2. Definir el alcance
3. Conformar el equipo de trabajo
4. Crear un plan de implementación
5. Realizar un análisis de brechas
6. Evaluar los riesgos

7. Implementar controles, procedimientos y programas de capacitación y sensibilización

8. Monitoreo y auditoría

Conclusiones, evidencias y muestras en la metodología de la investigación, técnicas e instrumentos.

Aplicación SGSI

Sistema de Gestión de la Seguridad de la Información, siendo para una empresa el proyecto de formación y el conjunto de conocimientos para formalizar de manera eficiente la facilidad a la información, tratando de certificar la reserva con honestidad, mostrando la disponibilidad de los activos de información, reduciendo a la vez los peligros de seguridad de la información (Valencia-Duque & Orozco-Alzate, 2017).

- **Confiabilidad:** Se reserva la información, sin revelar los procesos no autorizados a personas naturales u entidades.
- **Probidad:** El Sostenimiento al cumplimiento de la información y conocimientos a los procesos.
- **Reserva:** La Orientación para la utilización de la encuesta a los sistemas de información según el proceso y procedimiento a la misma por parte de las personas u entidades cuando lo requieran.

Objetivo del SGSI

El único objetivo es implantar y conservar un ambiente convenientemente, positivo y organizado a su gestión, de manera tal que permita preservar sus activos de información, así como un adecuado uso de los recursos y de la gestión del riesgo, con el fin de certificar la reserva, integridad y confiabilidad de la información que administra, así como la continuidad de los servicios tecnológicos que brindan a la institución. (Solarte et al., 2015).

Metodología

Para la obtención del estudio de caso, se utilizó como métodos, técnicas e instrumentos de investigación para lo cual se recopiló la información, y dio los siguientes resultados:

Investigación Cuantitativa

Mediante la investigación se consigue las mediciones numéricas o estadísticas conceptuando en probabilidades lógicas de acuerdo a los resultados que arrojaron las encuestas que fueron aplicadas al personal de la empresa.

Investigación Exploratoria

Se utilizó para este proyecto, la investigación exploratoria, debido a que se buscó cuáles fueron las causas del problema que está teniendo la empresa, conocer más a fondo de manera detallada cada una de ellas y de tal forma poder cubrir las necesidades de la mejor manera posible.

Técnicas de la investigación

Aplicando la encuesta, como una de las técnicas de investigación social desarrollando su uso en el campo de la investigación.

Instrumento

El instrumento para la obtención de datos en esta investigación fue el Cuestionario. El cual estuvo constituido por preguntas que me permitieron obtener información acerca del proceso de manejo de la información de esta organización (Anexo1).

Fundamentación de muestra teórica y variables como tema de investigación.

Seguridad de los servicios de redes ISO 27001

• Se deberá establecer que todos los sistemas y servicios de red estarán actualizados con recomendaciones de los fabricantes para asegurar los niveles óptimos de control y seguridad

La seguridad de los servicios de redes deberá implementarse según los lineamientos formales y definidos.

Procedimientos y políticas de transferencia de información ISO 27001

Acuerdos sobre transferencia de información ISO 27001

Toda la información en formato impreso o electrónico que sea utilizada entre organizaciones o usuarios externos, deberá estar bajo normativas de un Acuerdo de Confidencialidad mutuo (Formato de Acuerdos de Confidencialidad para Terceros), donde quedarán especificadas las responsabilidades para cada una de las partes.

Se deberán realizar evaluaciones de riesgos y seleccionar los controles adecuados para proteger la información involucrada en las aplicaciones gratuitas en las redes públicas.

• Para asegurar los servicios de aplicaciones en redes públicas se deben seguir los lineamientos formales.

Se debe elaborar, mantener y aplicar un procedimiento para la incorporación de sistemas de información, el cual debe incluir lineamientos, procesos, buenas prácticas, plantillas y guías que sirvan para regular los desarrollos de productos de software internos en un ambiente de aseguramiento de calidad.

Los productos de software adquiridos a través de terceras partes deben cumplir con los lineamientos formales de incorporación de sistemas de información establecidos.

• Deberá realizarse estrictamente la supervisión de los contratos y seguimiento de las actividades de desarrollo de software desarrollado por terceros

6.10.10. Pruebas de seguridad del sistema [ISO 27001 Cl A.14.2.8

• Las pruebas de aceptación se deben realizar en un ambiente de pruebas separado del ambiente de producción

• Las pruebas que usen los datos de producción deberán ser filtradas para no exponer información crítica. Se deben definir los procedimientos para el uso de la información requerida

El correo electrónico de la empresa deberá ser usada solo con fines de interés dentro de la Empresa.

Los administradores de servidores, bases de datos y demás roles que manejen información clasificada como confidencial, deben garantizar la confidencialidad de la información y el uso de credenciales de administración (usuario y contraseña), sin excepción.

• La presente política debe estar soportada por procedimientos formales y responsabilidades definidas.

Procedimiento de Gestión de Incidentes de Seguridad de la Información.

• El Plan de Contingencias Informático debe recibir mantenimiento para que se encuentre actualizado al momento de ser probado y se encuentre apegado a la realidad de las operaciones en la Empresa.

Privacidad y protección de datos personales ISO 27001

• Los registros de personal y sus datos privados deberán almacenarse en lugar seguro para evitar robo de información privada que pueda afectar la integridad del personal.

Cumplimiento de las políticas y normas de seguridad ISO 27001

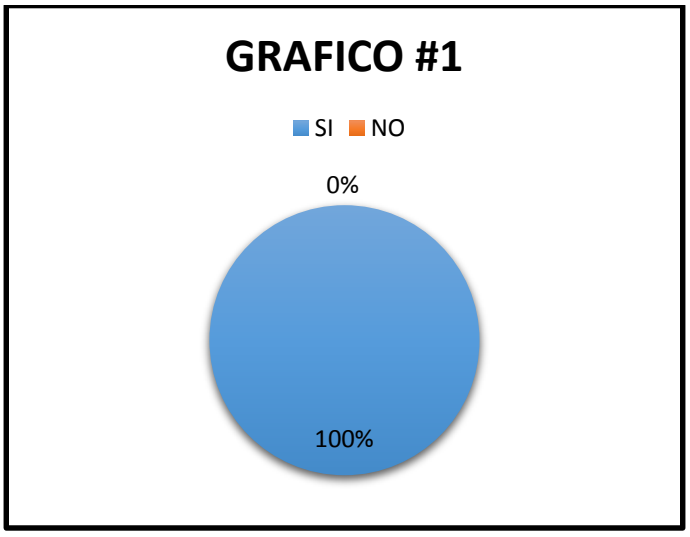
• El Oficial de Seguridad de la Información en conjunto con el Comité de Gestión de Seguridad de la Información son responsables del cumplimiento de todas las directivas, normas, procedimientos y estándares definidos.

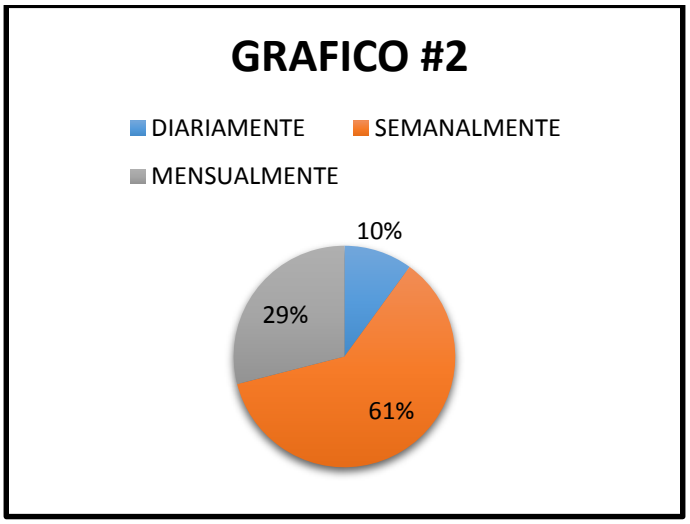
1.1Población y muestra

Normalmente la muestra se calcula utilizando la ecuación estadística denominada formula finita para determinar la población de una cantidad conocida, pero dado que la población en la organización estudiada es muy reducida, se decidió encuestar a todo el personal.

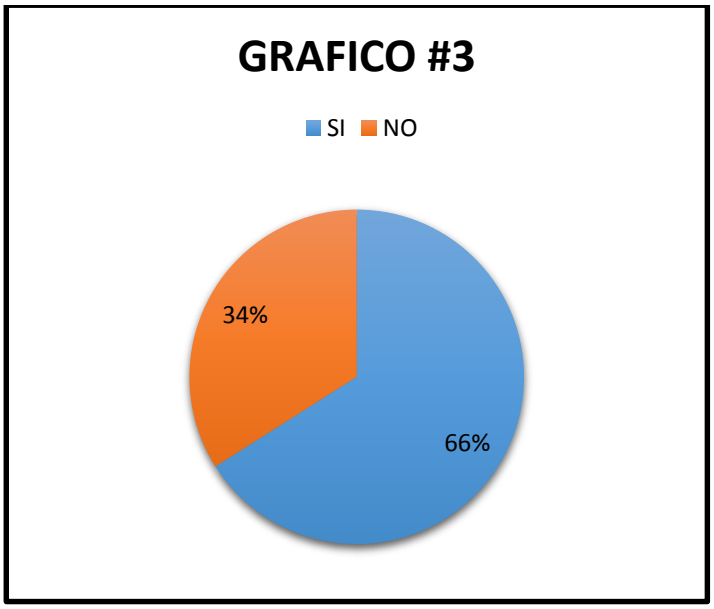
Resultados

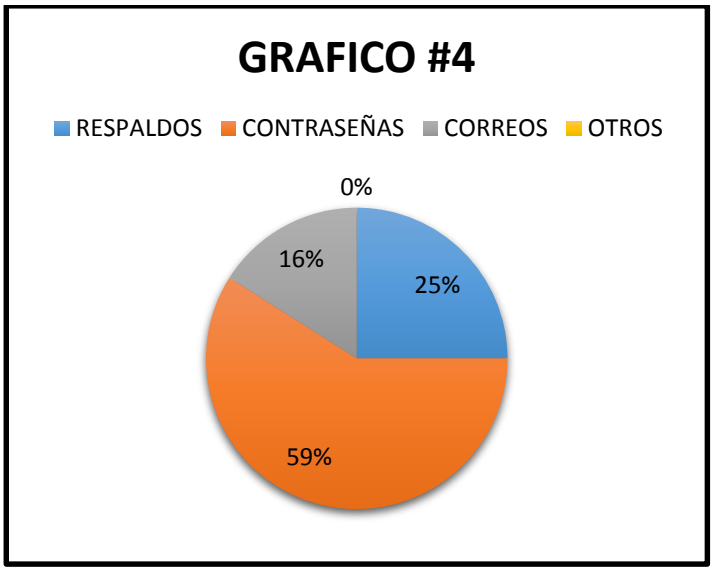
En los gráficos 1 y 2 se presentan los resultados obtenidos sobre las preguntas referentes a acceso a la información y a la frecuencia con que se respalda la misma, de ellos se obtuvo que el 100% respondió que solo personas autorizadas tienen acceso a la información; y con respecto a la frecuencia con que se respalda la información se obtuvo que el 61% respalda a semanalmente, el 29% respalda a mensualmente y el 10% respalda a diariamente.



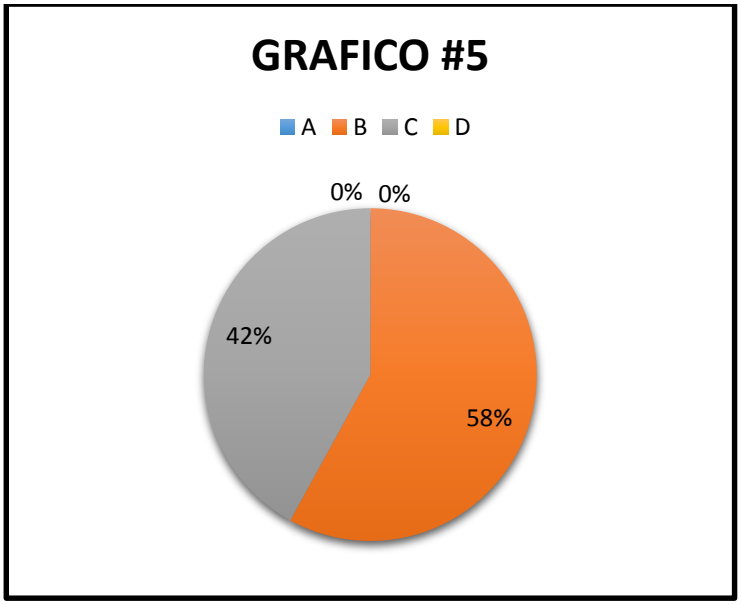


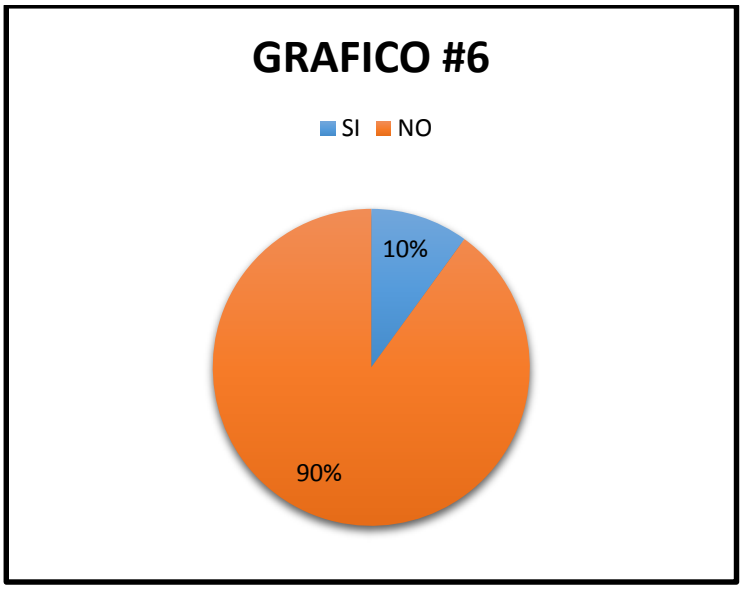
En los gráficos 3 y 4 se muestran los resultados obtenidos a partir de lo que respondieron los encuestados, referentes a las sobre la periodicidad del mantenimiento de los equipos informáticos y control de la información en el sistema; donde se obtuvo que el 66% respondió que si sobre el mantenimiento periódico de los equipos y el 34% respondió que no. Asimismo en relación con respecto al control de la información en el sistema el 59% respondió que es con contraseñas, el 25% respondió que es con respaldos y el 16% respondió que es con correos



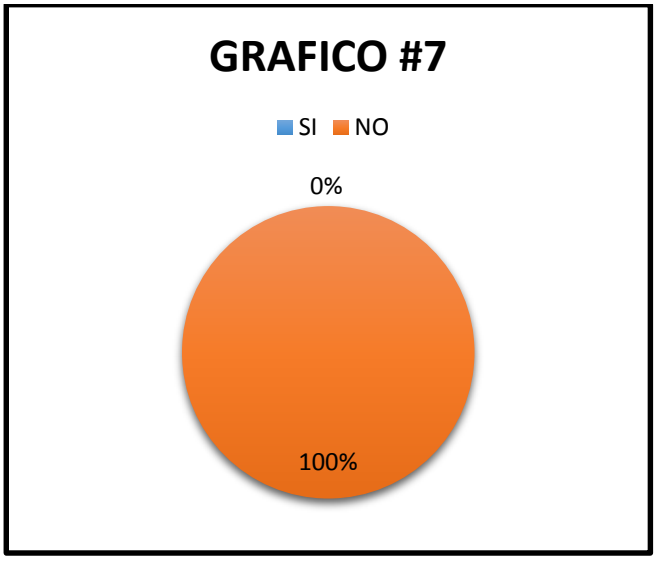


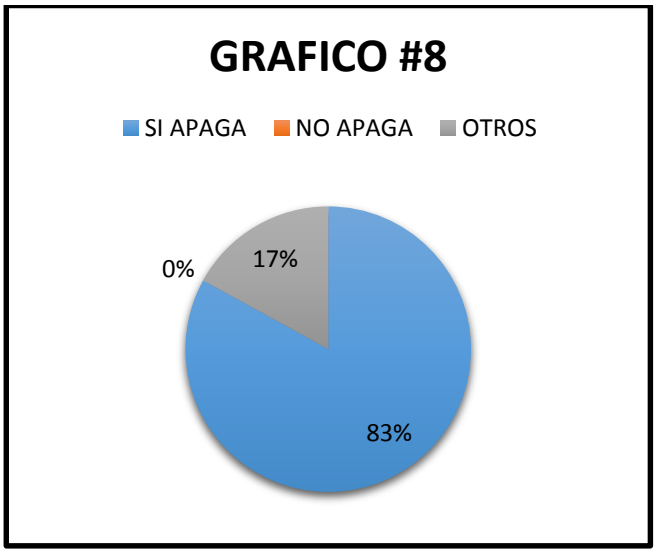
Los gráficos 5 y 6 muestran los resultados de la pregunta páginas web visitas por el personal en horas de trabajo; y si realizan o no algún tipo de descarga referente a archivos, donde se obtuvo como resultado que el personal visitan en un 58% tiendas online y proveedores, y que en un 42% visitan tiendas online y noticias, de esta manera podemos determinar que un 90% del personal no realizan descargas de archivos y el 10% no realiza esta actividad



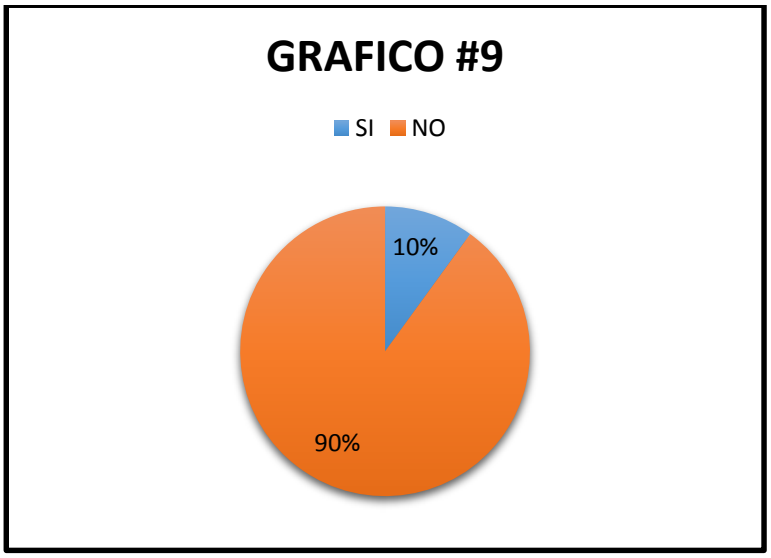


Los resultados de las preguntas 7 y 8 se muestran en los gráficos correspondientes, esto concernientes al registro de asistencia al personal y si al terminar sus labores apagan o dejan encendida la PC; de tal forma que un 100% del personal contestó no registrar su asistencia diaria a sus labores a esto se agrega que 83% del personal dice que apagan los equipos y un 17% en otros lo que equivale que el equipo queda en otras actividades.





Finalmente en el grafico 9 se exponen los resultados sobre conocer o no la norma ISO 27001 en la cual el 90% del personal no tienen conocimiento de dicha norma y el 10% constató que si tiene conocimiento.



CONCLUSIONES

Indudablemente la organización empresarial donde se realizó este trabajo carece de una estructura institucional y de patrimonios para el control y seguridad de la información.

La empresa debe considerar las actualizaciones respectivas de todos los procesos y equipamiento que comprometen las labores diarias de la empresa, asegurando su alta competitividad.

Para garantizar la confiabilidad y potenciar la competitividad, la empresa debe adoptar las políticas de seguridad que brinda la norma ISO 27001.

BIBLIOGRAFIA

Ascanio, J. G. A., Trillos, R. A. B., & Bautista, D. W. R. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. *Tecnura*, *19*(46), 123-134.

Basantes, J. B. Q., & Bahamonde, J. P. P. (2017). Beneficios de la aplicación de normas internacionales en procesos electorales. *Revista de Derecho Electoral*, (23), 3.

Bracho-Ortega, C., Cuzme-Rodríguez, F., Pupiales-Yépez, C., Suárez-Zambrano, L., Peluffo-Ordóñez, D., & Moreira-Zambrano, C. (2017). Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio. *Maskana*, *8*, 307-319.

Melo, V., & Hernando, A. (2008). El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27 001. *Revista de derecho*, (29), 333-366.

Ramos, M. A. (1996). La auditoría informática. *Informática y derecho: Revista iberoamericana de derecho informático*, (12), 983-992.

Ruíz Tapia, J. A., Estrada Gutiérrez, C. E., & Sánchez Paz, M. D. L. L. (2020). Propuesta de un Modelo de un Sistema de Gestión de Calidad en Seguridad de la Información basado en la norma ISO 27001 para Instituciones Educativas. *Revista de Investigación Latinoamericana en Competitividad Organizacional*, (febrero).

Sánchez-Henarejos, A., Fernández-Alemán, J. L., Toval, A., Hernández-Hernández, I., Sánchez-García, A. B., & de Gea, J. M. C. (2014). Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. *Atención Primaria*, *46*(4), 214-222.

Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL*, *28*(5).

Soto, M. D. C. S., Millán, N. D. C. O., Caro, M. S., & Garfias, J. I. M. (2017). La Auditoría Informática en las organizaciones. *Revista Electrónica Sobre Cuerpos Académicos y Grupos de Investigación*, *4*(8).

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação*, (22), 73-88.

ANEXOS

Anexo 1:


INTEROP


BuyNow
amazon


BuyNow
amazon
Hurley

Anexo 2:

Encuesta dirigida al personal de la Empresa Buy Now de la ciudad de Babahoyo.

El objetivo de esta encuesta es para determinar las falencias sobre seguridad informática que se encuentran en dicha empresa.

1. ¿Se ha permitido el acceso a la información sólo a personas debidamente autorizadas?

   a) SI ( )
   b) NO ( )

2. ¿En qué intervalo de tiempo usted respalda la información y datos que maneja la empresa?

   a) Diariamente ( )
   b) Semanalmente ( )
   c) Mensualmente ( )

3. ¿Se realiza un mantenimiento informático periódico sobre los equipos de la empresa?

   a) SI ( )
   b) NO ( )

4. ¿Qué tipo de control se utiliza para que los usuarios no modifiquen información del sistema de un modo no autorizado?

a) Respaldos ( )
b) Contraseñas ( )
c) Correos ( )
d) Otros ( )

5. ¿Qué tipo de páginas visita regularmente en sus horas de trabajo?

a) Tiendas Online ( )
b) Tiendas Online y Otros Proveedores ( )
c) Tiendas Online y Noticias ( )
d) Tiendas Online, Otros Proveedores y Noticias ( )

6. ¿Se utilizan programas de descarga de archivos de usuario, ya sean estos: Música, películas, programas, etc.?

a) SI ( )
b) NO ( )

7. ¿Registra usted su asistencia diaria al trabajo?

a) SI ( )
b) NO ( )

8. ¿Al terminar sus labores diarias, usted apaga la PC?

a) SI APAGA ( )
b) NO APAGA ( )
c) OTROS ( )

9. ¿Conoce usted acerca de la norma ISO 27001?

a) SI ( )
b) NO ( )