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(A) SISTEMAS

TEMA:

ANÁLISIS DEL DESARROLLO DE LOS SISTEMAS INFORMÁTICOS APLICANDO LA NORMA ISO 27001 EN LA EMPRESA MOSS SOLUTIONS

EGRESADA(O):

MURILLO GARCÍA ALVARO FABRICIO

TUTOR:

ING. RAÚL RAMOS

AÑO 2020

INTRODUCCIÓN

Los Sistemas informáticos en la actualidad son el punto clave para las empresas ya que en ellos se lleva el control de la organización, por eso la importancia de la realización de este caso de estudio con el tema: "ANALIZAR EL DESARROLLO DE LOS SISTEMAS INFORMATICOS SI ESTAN EN CUMPLIMIENTO CON LA NORMA ISO 27001 EN LA EMPRESA MOSS SOLUTIONS".

La empresa MOSS SOLUTIONS se dedica a la elaboración de sistemas es por ello que se realiza este trabajo investigativo para analizar la seguridad del software que allí se desarrolla, ya que muchas empresas en la ciudad de Babahoyo los han adquirido, por ello con este trabajo, se espera determinar la seguridad que tienen los clientes de estos sistemas con la filtración de información dando a conocer la exactitud de la seguridad que integran los sistemas. Moss Solutions tiene sistemas desarrollados que ya se encuentran en producción y otros en proceso de desarrollo los cuales serán analizado, para evaluar si está en cumplimento con las medidas de seguridad bajo la norma ISO/27001, esta va de la mano con otras normas que son necesarias para su implementación en los sistemas, ya que los datos que se ingresan son muy confidenciales y muy importante para el funcionamiento de las empresas, el presente tema tiene como finalidad dar a conocer la seguridad de los avances tecnológicos que se están desarrollando en la ciudad de Babahoyo de parte de la empresa Moss Solutions.

DESARROLLO

Moss es una empresa de soluciones informáticas que ofrece servicios de software, videovigilancia, biométrica, ciberseguridad y redes de datos con sede en Babahoyo.

La plataforma de programación Moss inició en 2009 por su fundador Manuel Espín que desarrolló una idea que consistía en la creación de una interfaz de sistema operativo de escritorio basado en Linux llamado Moss Optimus. El éxito lo llevó a mostrar su proyecto a alumnos y maestros a nivel nacional en una feria de Ciencia y Tecnología desarrollada por la Senescyt en Quito durante el mismo año en donde su proyecto obtuvo el primer lugar en el área de Informática y segundo lugar a nivel nacional. Moss Optimus sigue en desarrollo con el objetivo de mostrar al mundo que es posible crear software de calidad en Ecuador. Moss Solutions posee todas las soluciones y servicios informáticos en la Ciudad de Babahoyo. Y tiene como Misión: Desarrollar servicios de tecnologías de Información innovadores, que contribuyan a la eficiencia de los procesos administrativos, académicos y de investigación a un costo asequible brindando las garantías necesarias para que nuestros productos funcionen de forma óptima y segura en hogares y oficinas en el país.

Análisis de Desarrollo de los Sistemas Desarrollados en la Empresa

Tabla 1: Análisis del Sistema Conto Dinners Desarrollado en la Empresa

Conto Dinners	
Metodología	Cascada
Herramientas	Visual Basic/SQL Yog/Crystal Reports
Compilación	Escritorio
Codificación	8 meses
Diseño	2 meses
Pruebas	Caja negra/Caja Blanca
Mantenimiento	Actualizaciones
Tiempo de vida útil	5 años

Elaborado por: Alvaro Murillo

Detalle:

Es una solución integral diseñada para la gestión de negocios de hostelería como restaurantes, bares, discotecas, pizzerías, catering, cafeterías, domicilios, y cualquier otro servicio de alimentación. Es una edición de Conto completamente ideada para dispositivos de pantalla táctil.

Este Sistema fue desarrollado para ayudar a agilizar el proceso de pedido u orden cuando existe aforo de clientes, permitiendo así reducir el tiempo que conlleva atender a un cliente, ya que la orden pasa directamente a sistema desde la mesa que se encuentra realizando el pedido.

Este sistema inicio con una versión de escritorio la cual era muy difícil de manejar y de manipular en el ambiente para el que fue diseñado y al momento de llevarlo a la versión táctil ocurrieron ciertas dificultades al tratar de adaptar el diseño que ya existía a una versión totalmente interactiva con el usuario

Tabla 2: Análisis del Sistema Conto Enterprise Desarrollado en la Empresa

Conto Enterprise	
Metodología	XP
Herramientas	Visual Basic/SQL Yog/Crystal Reports
Compilación	Escritorio
Codificación	5 meses
Diseño	1 mes
Pruebas	Caja negra/Caja Blanca
Mantenimiento	Actualizaciones
Tiempo de vida útil	2 años

Elaborado por: Alvaro Murillo

Detalle:

Es una solución integral diseñada para tener control total de su negocio de comercio como boutiques, joyerías, perfumerías, supermercados, tiendas, almacenes, jugueterías, librerías, papelerías y demás, es fácil de utilizar, con un diseño muy visual e intuitivo, le permite realizar la lectura de artículos con códigos de barra, tener control y gestión de inventario, la fácil búsqueda de artículos por descripción será su mejor aliado.

Este sistema es la primera versión de sistema informático de escritorio desarrollado por la empresa, pero antes de su última actualización era conocido como Conto Comercial el cual es la plataforma base de sistemas que se fueron desarrollando después, en este sistema los desarrolladores fueron puliendo sus técnicas de programación aprendiendo nuevos códigos y herramientas para un correcto funcionamiento del sistema.

Tabla 3: Análisis del Sistema Conto Distbend Desarrollado en la Empresa

Conto Distbend	
Metodología	Cascada
Herramientas	Visual Basic/SQL Yog/Crystal Reports
Compilación	Escritorio
Codificación	8 meses
Diseño	2 mes
Pruebas	Caja negra/Caja Blanca
Mantenimiento	Actualizaciones
Tiempo de vida útil	5 años

Elaborado por: Alvaro Murillo

Detalle:

Es una solución integral diseñada para tener control total de la distribuidora Distbend, es una versión personalizada a los requerimientos del cliente, permite el control de ventas, retenciones, proformas etc. También emite reportes y estados de cuentas, en este sistema uno de los problemas fue que el cliente no establecía exactamente los requerimientos que necesitaba, lo cual dificulto un poco el desarrollo.

Tabla 4: Análisis del Sistema Web Integra Desarrollado en la Empresa

Integra	
Metodología	XP
Herramientas	Php/phpmyadmin/html/Servidor online
Compilación	Web
Codificación	3 meses
Diseño	1 mes
Pruebas	Caja negra/Caja Blanca
Mantenimiento	Actualizaciones
Tiempo de vida útil	2 años

Elaborado por: Alvaro Murillo

Detalle:

Es una aplicación web que se encuentra desarrollada para la propia empresa de Moss Solutions la cual lleva un control de facturas, garantías, clientes etc.

El sistema integra es la actualización del sistema scalable en la cual tenía errores con la versión antigua de Php.

Sistemas informáticos

Los Sistemas informáticos se han convertido en una herramienta fundamental en cualquier ámbito de la sociedad actual.

> Con el rápido desarrollo de las tecnologías electrónicas, diariamente se crean multitud de dispositivos. Este hecho, unido a la creciente necesidad de comunicación, hace necesaria la cualificación de profesionales en el sector de los sistemas de telecomunicaciones e informáticos. Esta Investigación va dirigido a estudiantes tanto de ciclos formativos como de universidad, un público en general interesado en la instalación y la configuración de sistemas informáticos y redes locales, así como a profesionales del sector. En concreto, para la formación profesional el módulo de sistema informáticos y redes locales forma parte del currículo del ciclo formativo de grado superior de sistemas de telecomunicaciones e informáticos pertenecientes a la familia profesional de electricidad y electrónica (MIRANDA, 2014) **.**

Definición de un SGSI

Un Sistema de Gestión de Seguridad de la Información (SGSI), según la Norma UNE-ISO/IEC 27001, es una parte del sistema de gestión general.

> Es basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información, esto significa que se va a dejar de operar de una manera intuitiva y se va a empezar a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización, nos permitirá conocer mejor nuestra organización,

cómo funciona y qué podemos hacer para que la situación mejore (Andrés & Gomez, 2009, p. 13).

Desarrollo de Sistemas De Información

Las Necesidades para el desarrollo de un sistema de información varían en función del tipo del Problema que se intenta solucionar, el número de personas que se ven afectadas.

las áreas del negocio en donde el sistema proporciona información, la relevancia del nuevo sistema según la estrategia del negocio, etc. Cada uno de los sistemas de información propuestos hasta el momento se puede desarrollar de distintas maneras.

Todos los sistemas de información que una organización decida mejor introducir deben desarrollarse completamente dentro de la empresa, si el problema es común dentro del sector, es posible que existan soluciones estandarizadas que ofrezcan una relación beneficios-coste que mejor que si se desarrolla internamente.

A continuación se enumeran distintos métodos de construcción de sistemas:

- Desarrollo basado en modelos.
- Desarrollo rápido de aplicaciones.
- Paquetes de software de aplicaciones.
- Desarrollo por parte del usuario final.
- Subcontratación. (Alarcón, 2010, p. 37)

Ciclo de vida en cascada

El ciclo de vida en cascada es la secuenciación de las distintas fases de la producción del software que se han descrito, como elementos de unión entre cada fase aparecen los diferentes docunentos que se generan en cada fase, en la figura se puede ver la organización de un ciclo de vida en cascada.

Cada fase se sepante clarentamente de la siguiente lo que permite la independización su realización, los elementos de unión entre las fases son sos documentos generados en las mismas, el modelo en cascada obliga a un terminar cada fase antes de comenzar con la siguiente. Cada fase fundamenta su trabajo en los espursos de la anterior, error de detectar para detectar posible y evitar que se propaguen a las fases de procesos se establecen procesos de revisión al complet fase, antes de pasar a la sigurnte esta revisión se realiza sobre la documentación generada en cada fase de manra formal siguyendo una lista de las comprobaciones establecida de anteno. Errores detectan de si se en una fase será necesario corregiros en esa fase y todos los puntos del ciclo de vida anteriores. (Gómez Palomo & Moraleda Gil, 2020, p. 37)

Figura 1. Ciclo de Vida en Cascada. Gómez Palomo & Moraleda Gil, (2020)

Modelo XP

El modelo XP La metodología XP define cuatro variables para cualquier proyecto de software: coste, tiempo, calidad y alcance.

De estas cuatro variables tres de ellas podrán ser fijadas arbitrariamente por actores externos al grupo de desarrolladores (clientes y jefes de proyectos). El valor de la variable restante podrá ser establecido por el equipo de desarrollo, en función de los valores de las otras tres.

Ejemplo: si el cliente establece el tiempo y la calidad, y el jefe de proyecto el coste, el grupo de desarrollo tendrá libertad para determinar la elalcance del proyecto (es decir, el número de historias de usuario que puede finalizar en dicho contexto). El ciclo de vida de un proyecto XP incluye, al igual que cualquier otra metodología, entender lo que el cliente necesita, estimar el esfuerzo, crear la solución y entregar el producto final al cliente. Sin embargo, XP propone, aligual que el resto de metodologías ágiles, un ciclo de vida dinámico, donde se admite expresamente que, en muchos casos, los elientes no son capaces de especiticar sus requerimien- tos al comienzo de un proyecto.

Diseñador de sistemas SI

Un Diseñdor de sistemas son los que estan encargado del desarrollo de los sistemas informaticos de acuerdo a los requerimientos de los clientes utilizando las nuevas tecgnologias que van surgiendo a medida que avanza el tiempo.

Métodos de encriptación

Algunos de los métodos de encriptación disponibles actualmente y que son bastantes conocidos se pueden mencionar a:

- Encriptación simétrica Encriptación asimétrica de clave pública y privada
- Encriptación WPA
- Encriptación WEP
- Firma digital

Estos métodos mencionados anteriormente son la mayoría que se va a encontrar en el mundo de la seguridad informática, estos métodos de encriptación son bastantes buenos para almacenar y transferir la información. métodos criptográficos (Castro, y otros, 2018, p. 23).

AES (o algoritmo de Rijndael)

En el año 2001, el algoritmo de Rijndael (WIKI AES) fue anunciado como nuevo estándar avanzado de cifrado para empleo de aplicaciones criptográficas no militares, potente, eficiente y fácil de utilizar (CRIPTO).

> Creado por los Belgas Joan Daemen y Vincent Rijmen, es un sistema de cifrado por bloques, diseñado para manejar longitudes de clave variable comprendidas entre 128 y 256 bits, Según sus autores, y basado en la estructura de su diseño, el método más eficiente conocido hasta la fecha para recuperar la clave a partir de un par texto cifrado texto claro, es la busqueda por fiverza bruta, por lo que se con sidera en la actualidad como uno de los métodos más seguros. (Sarubbi, 2008, p. 49)

Tecnica de Pruebas

En el ámbito de la ingeniería de software, toda actividad se guía por la aplicación de técnicas: Procedimientos técnicos o de gestión que ayudan a ejecución, evaluación y mejora de los procesos de desarrollo de software (IEEE,1990).

> Las técnicas más comunes aplicadas en los procesos de prueba tienen el objetivo de seleccionar buenos casos de prucba, esto es. casos que tengan una probabilidad alta de descubrir un error tradicionalmente (Myers, 2004, Beizer, 1990) se han considerado dos enfoques complementarios para seleccionar casos de prueba, denominados caja blanca y caja negra.

Pruebas de caja blanca

> Existen varias estrategias que permiten obtener casos de prueba a partir del código fuente de un programa (Beizer, 1990).
>
> Las siguientes son algunas de las más representativas:

- Cobertura de código: Su objetivo es elegir casos de prueba de modo que una determinada propiedad o característica del código tome el mayor número posible de valores.
- Pruebas de bucles: Se basan en seleccionar casos en los que los bucles se ejecutan de diferentes maneras. Por ejemplo, pueden plantearse pruebas en las que el cuerpo de un bucle sólo se ejecuta una vez o bien un nůmero máximo de veces.
- Flujo de datos: Esta estrategia se basa en elegir casos de prueba en cuya ejecución una variable determinada, o en general una estructura de datos, toma diferentes valores.

Pruebas de caja negra

Frente a las técnicas de prueba de caja blanca, las técnicas de caja negra seleccionan casos de prueba a partir de las especificaciones funcionales del software (Beizer, 1995). Pueden aplicar, por tanto, cuando aún no está implementado el código fuente del programa pero si se conoce lo que se espera que haga, existen varios enfoques, complementarios, para realizar este tipo de pruebas, de los que se mencionan aquí los más relevantes:

- Partición del sistema: Consiste en realizar una división del dominio de entrada en particiones para las que se supone un mismo comportamiento y utilizar cada una de ellas para seleccionar casos de prueba.
- Pruebas sobre los estados del software: Se obtienen casos de prueba que ejerciten los diferentes estados en los que pueden estar el software, por ejemplo, el carrito de la comparación de una tienda virtual podría estar en el estado "pagado" o "pendiente de entrega".

- Pruebas del flujo lógico de control: Con este enfoque, los casos de prueba se especifican como un conjunto de operaciones que deben realizarse consecutivamente sobre el software bajo prucba. (Ramos Román, Dolado Cosín, & Tuya, 2007)

Historia de la Norma ISO

La Organización Internacional para la Normalización ISO (Organización Internacional de Normalización), fue establecida en Ginebra en 1946 con el propósito de estandarizar productos industriales y de consumo que son comercializados internacionalmente.

> Nació para asegurarse que las tuberías son del mismo grosor, las telecomunicaciones usaran las mismas bandas, etc. Su misión fundamental es facilitar el comercio de bienes y servicios, las decisiones de estandarización técnica son internas a la industria. ISO se convirtió en el organismo internacional para el establecimiento de normas, trabajando con cuerpos nacionales de normalización, ingenieros de departamentos de gobierno y representantes de la industria, particularmente con corporaciones transaccionales para quienes este aspecto es crucial los estándares creados representan un consenso internacional de excelencia. (state of the art).
>
> ISO desarrolla los estándares que el mercado requiere, en su constante búsqueda por satisfacer esas necesidades de mercado, en los años ISO diversificó sus operaciones creando estándares en el área administrativa: gestión total de la calidad el resultado de esta acción fue el proceso de certificación que indica que una organización se desempeña bajo las pautas de calidad total Serie ISO 9000 (Cordero, 2004, p. 94).

La Politica, las Normas y los Procedimientos en seguridad de sistemas

La política de seguridad refleja la postura adoptada por la empresa en relación a la confidencialidad, disponibilidad e integridad de los datos, programas, equipos, personal, relacionados con los SI de dicha empresa.

La asignación de medios para la seguridad dependiente de la mencionada política.

Algunas características a cumplir son:

- Ser de cumplimiento obligatorio por todos los entes relacionados con los SI; por tanto, será publicado a todos los niveles de la entidad.
- Plasmarse en un documento escueto (no más de 2-3 páginas). Estar apoyada por la dirección, para lo cual esta debe estar concienciada y sensibilizada.
- Ser genérica, no obligando a revisiones constantes.
- Las revisiones es recomendable realizarlas cada 3-5 años.
- Incluir los requisitos mínimos (Heredero, Agius, Romero, & Salgado, 2019).

ISO/ICE 27001

Esta es la versión actual de la especificación estándar para el sistema de gestión de seguridad de la información.

Es independiente del proveedor y de la tecnología, está destinado a ser aplicado por empresas de cualquier tipo, tamaño o naturaleza y en cualquier industria de todo el mundo “por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro” es un sistema de gestión, no una especificación tecnológica, con el título formal de tecnología de la información (TI) - Técnicas de seguridad - sistemas de gestión de seguridad de la información - requisitos. pertenece a una familia mucho más compatible que consta de una serie numerada de estándares internacionales para la

gestión de la seguridad de la información de los cuales ISO / IEC 27000 es el estándar básico (Calder, 2017, p. 13).

Controles de la ISO 27001

Esta norma específica los requisitos necesarios para el establecimiento, implantación, mantenimiento y mejora de un sistema de gestión para la seguridad de la información (SGS).

Utiliza como herramienta el "Ciclo de Deming" o PDCA (Plan-Do -Check - Act). La organización que se certifica en esta ISO adquiere competencia competitiva sobre las que no, puesto que con esta certificación demuestra que:

- Los controles de seguridad internos se realizan de forma independiente.
- Que cumple los requisitos de la gestión corporativa.
- Que cumple los requisitos relativos a la continuidad de la actividad comercial.
- Que se respetan las leyes y normativas de aplicación al respecto.
- Que se cumplan los requisitos contractuales.
- Que la seguridad de la información constituye una prioridad en su plan de empresa (Calvo, 2015, p. 350).

Seguridad, registro y confidencialidad de la información y la comunicación

Seguridad, registro y confidencialidad de la información y la comunicación todo lo referente a la normativa legal sobre seguridad, registro y confidencialidad de la información y la comunicación la veremos en el siguiente apartado.

Ahora vamos a pasar a ver la norma ISO, que son una noma que nos indica como realizar una gestión correcta y de calidad sobre un proceso determinado, 27001. La norma iso 27001 sirve para la seguridad de la información basada en la preservación de su confidencialidad, integridad y disponibilidad, disponiendo de los sistemas implicados en

su tratamiento, dentro de la organización, para que la gestión de la seguridad de la información sea correcta debemos identificar el ciclo de vida de la misma en la organización y sus aspectos relevantes:

- Confidencialidad: La no disposición ni revelación de la información a personas, entidades o proceso no autorizado.
- Integridad: La preservación de la exactitud y la completitud de la formación y sus métodos de proceso.
- Disponibilidad: La disposición y utilización de la información y los sistemas de tratamiento a personas, entidades o procesos autorizados cuando requieran (Pradillo, 2015, p. 78).

ISO 27002,

La Introducción (Cláusula 0) de ISO / IEC 27002: 2013 (ISO 27002), el código internacional de mejores prácticas para ISMSS, respalda este enfoque empresarial y orientado al riesgo.

Los recursos empleados en la implementación de controles deben equilibrarse con los daños que probablemente resulte de problemas de seguridad en ausencia de esos controles, los resultados de una evaluación de riesgos ayudarán a guiar y determinar la acción de administración apropiada y las prioridades para administrar los riesgos de seguridad de la información y para implementar los controles seleccionados para proteger contra estos riesgos.

Un número creciente de organizaciones está adoptando este enfoque para la gestión del riesgo, a lo largo de los años, han surgido una serie de estándares nacionales o patentados que se ocupan de la gestión de riesgos de seguridad de la información, todos tienen

> mucho en común. ISO 27001 es la norma internacional que establece los requisitos para un SGSI y proporciona un enfoque para la gestión de riesgos consistente con todas las demás guías, de hecho, muchos de los otros marcos que están disponibles se basan en ISO 27001. (Calder & Watkins, 2019, p. 11)

La ISO 27001 especifica los 114 controles que se pueden usar para reducir los riesgos de seguridad mientras que la ISO 27002 proporciona información de como estos deben aplicarse.

ISO/ICE/27005

La ISO 27005 establece las directrices para la gestión del riesgo de seguridad de la información, además de que también apoya los conceptos generales especificados en la norma ISO/IEC7001.

> Está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en el enfoque de gestión de riesgos, el conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de seguridad de la Información (Urbina, 2016, pp. 48;49).

Control de Seguridad

El acceso a los sistemas informaticos que desarrolla la empres Moss Solutions se encuentra encriptada a nivel de base de datos, la cual no puede ser alterada o visualizada mediante el acceso al gestor de base de datos, ya que ningun usuario final tiene las credenciales de acceso al mismo.

Análisis de riesgos de seguridad.

En ambiente de los Sistemas Informáticos, son varios los recursos como por ejemplo técnicos, organizativos y gestión, todos estos tipos son riesgos que están expuestos a riesgos ya sean en una organización o empresa en especial los sistemas informáticos que son los ricos en información muy importante ya que la mayoría de los sistemas son contables y llevan la contabilidad de estas, ya que existen personas maliciosas con mentalidad de lucrarse o causar perjuicio a la empresa.

CONCLUSIONES

los Sistemas en la empresa Moss Solutions se desarrollan bajo una metodología siguiendo el lineamiento correcto para el desarrollo óptimo para su correcto funcionamiento pasando por los niveles de pruebas y su debido mantenimiento.

De acuerdo la información obtenida mediante la encuesta realizada a los encargados de desarrollo de la empresa podemos determinar que si tienen el conocimiento y están aplicando las normas mencionadas en mi investigación lo cual la empresa aprobaría con lo referente a tema de seguridad y desarrollo de sistema e información de los clientes.

La norma ISO 27001 es la que se encarga de analizar y evaluar los riesgos basados en los procesos. evalúa y controla a la organización en relación a los diferentes riesgos a los que se encuentra sometido el sistema de informáticos.

Es necesario implementar buenas prácticas que permitan establecer controles para proteger las características de la seguridad de la información, existen diversas herramientas privadas que apoyan el sistema de gestión de seguridad de la información, optimizando procesos o actividades.

La Norma ISO 27002 es la encargada de gestionar y guiar los procesos de los controles para la ejecución de la evaluación de la Norma ISO 27001 bajo una evaluación de cumplimiento los controles

REFERENCIAS

Alarcón, V. F. (2010). *Desarrollo de Sistemas de Información una Metodología Basada en el Modelado.* Catalunya.

Andrés, A., & Gomez, L. (2009). *Guía de aplicación de la a Norma UNE-ISO/IEC 27001 sobre seguridad de información para pymes.* españa: AENOR.

Calder, A. (2017). *ISO27001/ISO27002: Una guía de bolsillo.* IT Governance Ltd.

Calder, A., & Watkins, S. (2019). *Information Security Risk Management for ISO 27001/ISO 27002, third edition.* IT Governance Ltd.

Calvo, N. d. (2015). *UF1643 - Gestión y control de los sistemas de Información.* España : Elearning, S.L.

Castro, M. I., Morán, G. L., Navarrete, D. S., Cruzatty, J. E., Anzúles, G. R., Mero, C. J., . . . Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Manabi: Area de Innovacion y Desarrollo,S.L.

Cordero, M. B. (2004). *Gestión ambiental: camino al desarrollo sostenible.* Universidad Estatal a distancia.

Gómez Palomo, S. R., & Moraleda Gil, E. A. (2020). *Aproximación a la ingeniería del software.* Centro de Estudios Ramon Areces SA.

Heredero, C. d., Agius, J. J., Romero, S. M., & Salgado, S. M. (2019). *Organización y transformación de los sistemas de información en la empresa* (4ta Edicion ed.). Madrid: esic.

MIRANDA, C. V. (2014). *SISTEMAS INFORMATICOS Y REDES LOCALES.* ESPAÑA: paraninfo S.A.

Pradillo, I. G. (2015). *MF0975_2 - Técnicas de recepción y comunicación* (6TA ed.). España : Elearning, S.L.

Ramos Román, I., Dolado Cosín, J., & Tuya, J. (2007). *Técnicas Cuantitativas para la Gestión en la Ingeniería del Software.* Netbiblo, S.L.

Sarubbi, J. P. (2008). *Seguridad informatice Tecnicas de defensa comunes bajo variantes del sistema Operativo Unix.* Argentina: Universidad de Lujan.

Urbina, G. (2016). *Introducción a la seguridad informática.* Mexico: Grupo Editorial Patria.

ANEXOS

La siguiente evaluación de controles fue realizada a las 2 personas que están encargadas del desarrollo de los sistemas en la empresa.

ANEXOS

Evaluación de Controles de la Norma ISO 27001

1. ¿Qué Tarea desempeña en el desarrollo de sistema?
   - Codificación. [ ]
   - Diseño. [X]
   - Otros. [ ] _____
2. ¿Los sistemas que usted ha desarrollado manejan inventario?
   - Si [✓]
   - No [ ]
   - Si es No Especifique su respuesta. _____
3. ¿Sus sistemas generan archivos referentes al funcionamiento del sistema que se puedan modificar?
   - Si [ ]
   - No [X]
4. ¿Qué Seguridad de información Utiliza al momento de establecer un sistema?
   - Respaldo de Datos [X]
   - Red Segura [X]
   - Autenticación Cifrada [X]
5. ¿Utiliza Cifrado en alguna Parte de Su Sistema?
   - Si. [X]
   - No. [ ]
6. ¿Sus sistemas Utilizan Facturación Electrónica?
   - Si [X]
   - No. [ ]
7. ¿Realizan una Copia de Seguridad de Información?
   - Si. [X]
   - No. [ ]
8. ¿Realizan separación de entornos de desarrollo, prueba y producción?
   - Si. [X]
   - No. [ ]
9. ¿Los Sistemas tienen Registros de actividad del administrador y operador del sistema?
   - Si. [X]
   - No. [ ]
10. ¿Exigen equipos Licenciados donde instalan los sistemas?
    - Si. [X]
    - No. [ ]

11. ¿Realizan el debido Análisis y especificación de los requisitos de seguridad a sus clientes?
    - Si. [X]
    - No. [ ]
12. ¿La Empresa tiene o cubre con Política de desarrollo seguro de software?
    - Si. [X]
    - No. [ ]
13. ¿Hacen uso de principios de ingeniería en protección de sistemas?
    - Si. [X]
    - No. [ ]
14. ¿Realizan las debidas Pruebas de funcionalidad durante el desarrollo de los sistemas?
    - Si. [X]
    - No. [ ]
15. ¿Hacen protección de los datos utilizados en pruebas?
    - Si. [X]
    - No. [ ]
16. ¿Realizan Notificación de puntos débiles de la seguridad a sus clientes?
    - Si. [X]
    - No. [ ]
17. Realizan Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
    - Si. [X]
    - No. [ ]
18. ¿los Sistemas desarrollados tienen Protección de datos y privacidad de la información personal?
    - Si. [X]
    - No. [ ]
19. ¿Protección de regulación de los controles criptográficos?
    - Si. [X]
    - No. [ ]
20. ¿Cumple con los Requisitos de Gestión Corporativa?
    - Si. [X]
    - No. [ ]

Ing. Manuel Espín
Gerente

ANEXOS

Evaluación de Controles de la Norma ISO 27001

1. ¿Qué Tarea desempeña en el desarrollo de sistema?
   - Codificación. [X]
   - Diseño. [ ]
   - Otros. [ ] _____
2. ¿Los sistemas que usted ha desarrollado manejan inventario?
   - Si [X]
   - No [ ]
   - Si es No Especifique su respuesta. _____
3. ¿Sus sistemas generan archivos referentes al funcionamiento del sistema que se puedan modificar?
   - Si [ ]
   - No [X]
4. ¿Qué Seguridad de información Utiliza al momento de establecer un sistema?
   - Respaldo de Datos [X]
   - Red Segura [X]
   - Autenticación Cifrada [X]
5. ¿Utiliza Cifrado en alguna Parte de Su Sistema?
   - Si. [X]
   - No. [ ]
6. ¿Sus sistemas Utilizan Facturación Electrónica?
   - Si [X]
   - No. [ ]
7. ¿Realizan una Copia de Seguridad de Información?
   - Si. [X]
   - No. [ ]
8. ¿Realizan separación de entornos de desarrollo, prueba y producción?
   - Si. [X]
   - No. [ ]
9. ¿Los Sistemas tienen Registros de actividad del administrador y operador del sistema?
   - Si. [X]
   - No. [ ]
10. ¿Exigen equipos Licenciados donde instalan los sistemas?
    - Si. [X]
    - No. [ ]

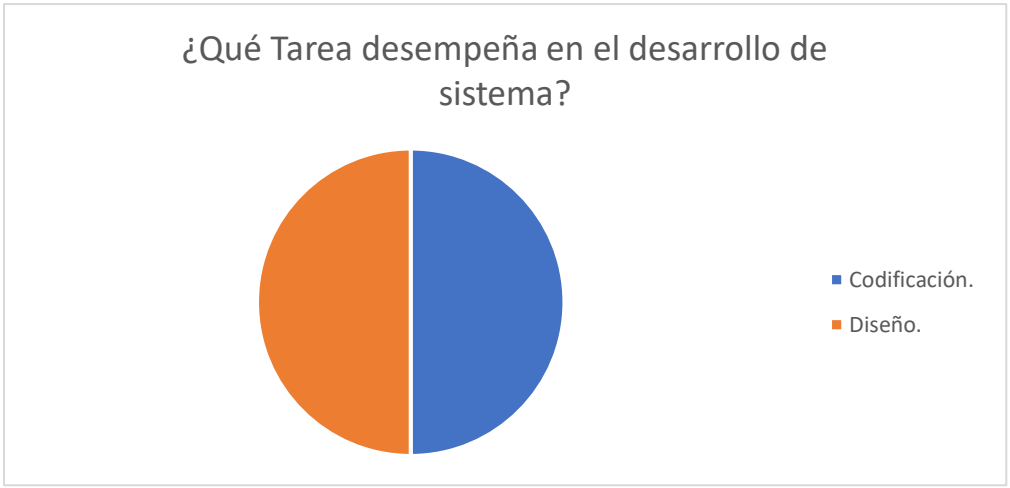
ANEXOS

Evaluación de Controles de la Norma ISO 27001

1. ¿Qué Tarea desempeña en el desarrollo de sistema?
   - Codificación. [X]
   - Diseño. [ ]
   - Otros. [ ] _____
2. ¿Los sistemas que usted ha desarrollado manejan inventario?
   - Si [X]
   - No [ ]
   - Si es No Especifique su respuesta. _____
3. ¿Sus sistemas generan archivos referentes al funcionamiento del sistema que se puedan modificar?
   - Si [ ]
   - No [X]
4. ¿Qué Seguridad de información Utiliza al momento de establecer un sistema?
   - Respaldo de Datos [X]
   - Red Segura [X]
   - Autenticación Cifrada [X]
5. ¿Utiliza Cifrado en alguna Parte de Su Sistema?
   - Si. [X]
   - No. [ ]
6. ¿Sus sistemas Utilizan Facturación Electrónica?
   - Si [X]
   - No. [ ]
7. ¿Realizan una Copia de Seguridad de Información?
   - Si. [X]
   - No. [ ]
8. ¿Realizan separación de entornos de desarrollo, prueba y producción?
   - Si. [X]
   - No. [ ]
9. ¿Los Sistemas tienen Registros de actividad del administrador y operador del sistema?
   - Si. [X]
   - No. [ ]
10. ¿Exigen equipos Licenciados donde instalan los sistemas?
    - Si. [X]
    - No. [ ]

Tabulación de resultados

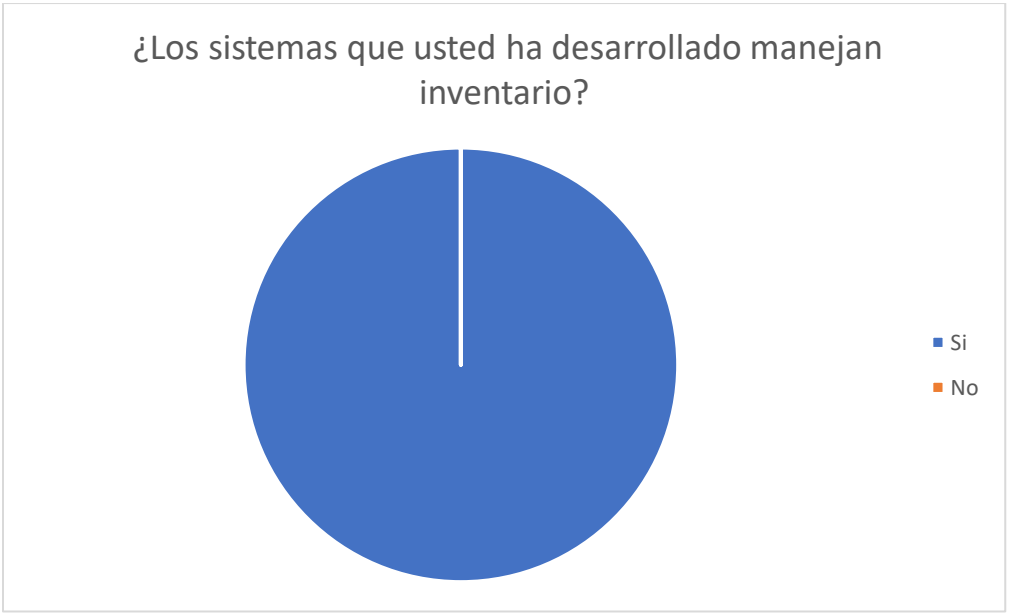
1. **¿Qué Tarea desempeña en el desarrollo de sistema?**



Observación:

En la empresa los encargados del desarrollo de los sistemas son 2 personas a las cuales se les aplico la evaluación y se dividen el trabajo en 50% ya que uno se encarga de la parte de codificación y la otra persona del diseño.

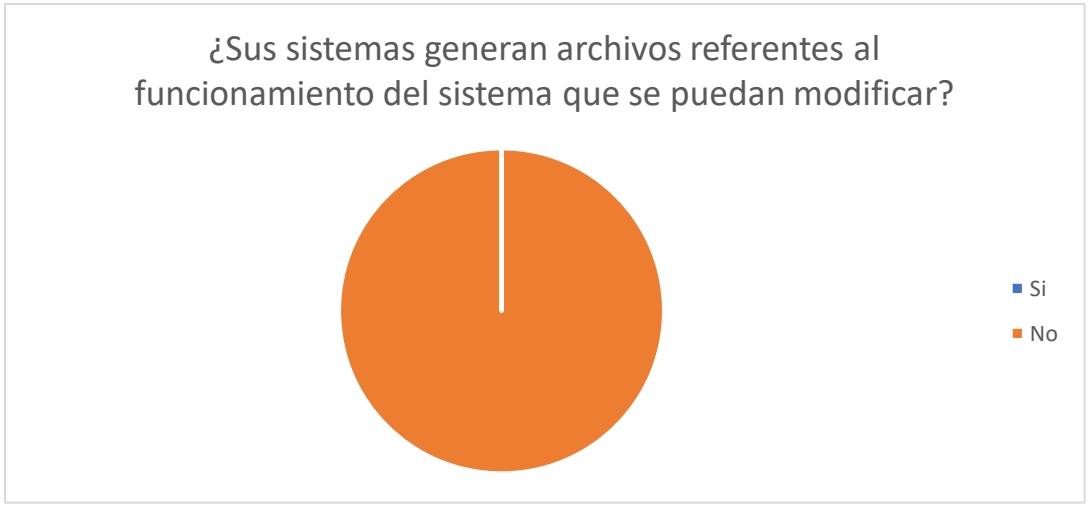
2. **¿Los sistemas que usted ha desarrollado manejan inventario?**



Observación:

La mayoría de sus sistemas manejan inventario, pero existen varios complementos que no manejan inventario dependiendo los requerimientos del cliente.

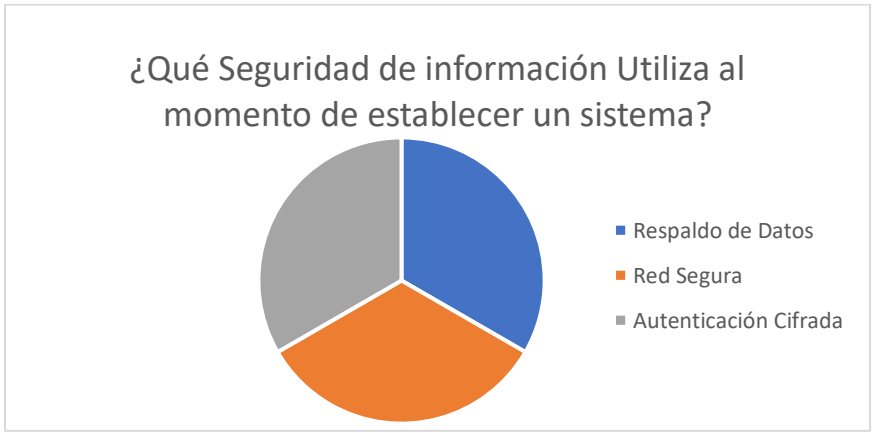
3. **¿Sus sistemas generan archivos referentes al funcionamiento del sistema que se puedan modificar?**



Observación:

Al momento de generar un archivo lo hace en formato XML que no se puede modificar ya se genera y se elimina en menos de 3 segundos para que no pueda ser modificado

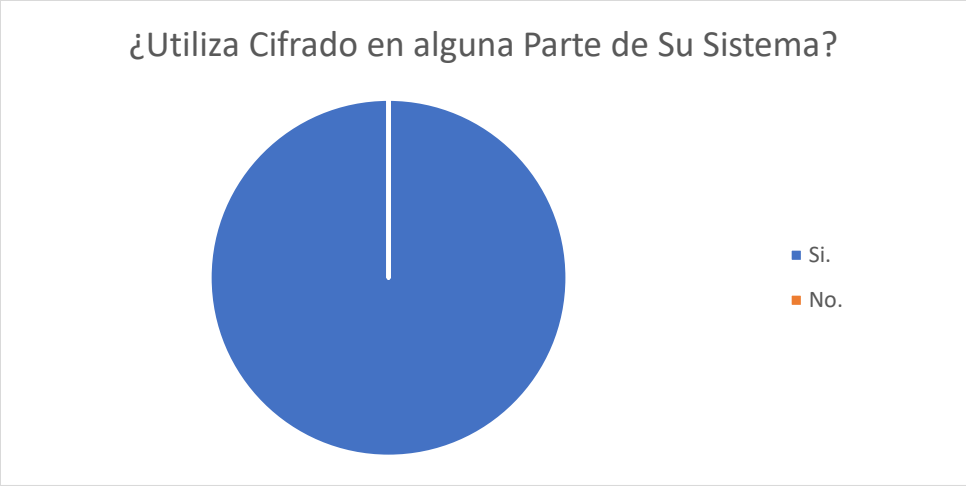
4. **¿Qué Seguridad de información Utiliza al momento de establecer un sistema?**



Observación:

El respaldo de datos se utiliza para almacenarlos en la nube en caso de perder información local se recupera, se utiliza la red segura para que nadie pueda ingresar de un equipo que esta fuera de la red y referente a la autentificación cifrada funciona en las contraseñas de los usuarios

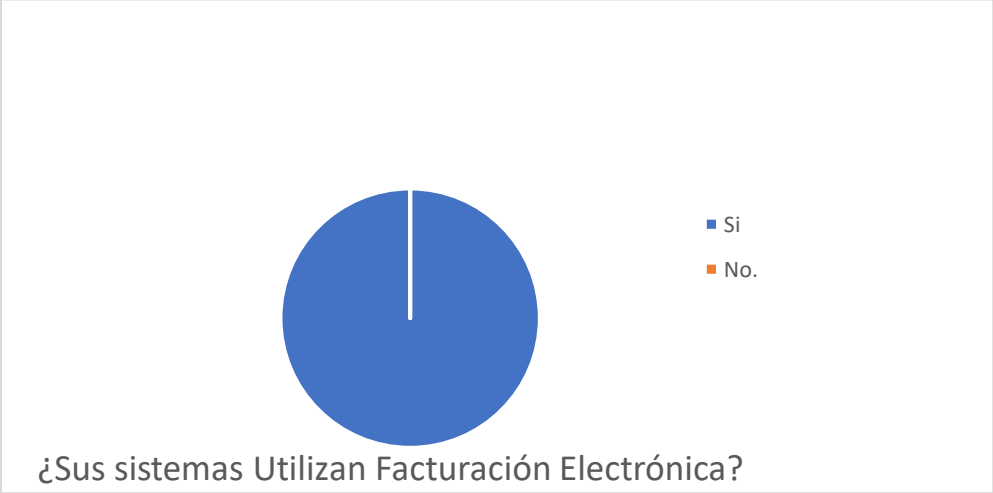
5. **¿Utiliza Cifrado en alguna Parte de Su Sistema?**



Observación:

Los datos del acceso se encriptan y se comparan a los datos de la base de datos para dar acceder al sistema

6. **¿Sus sistemas Utilizan Facturación Electrónica?**



Observación:

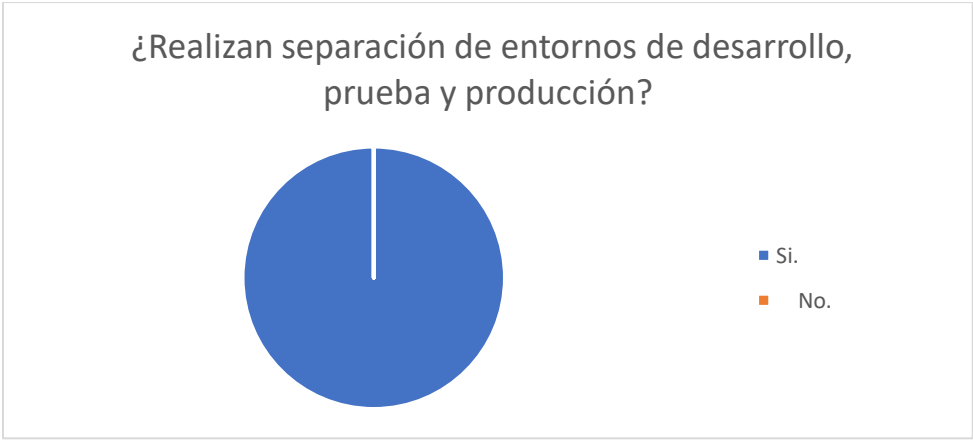
Para los clientes que están obligados a llevar contabilidad si ya que al momento de hacer las declaraciones las facturas ya se encuentran en el SRI

7. **¿Realizan una Copia de Seguridad de Información?**

Observación:

Si, Realiza una copia de seguridad y se almacena en la nube con la herramienta Dropbox que es un servidor de alojamiento fuera del país.

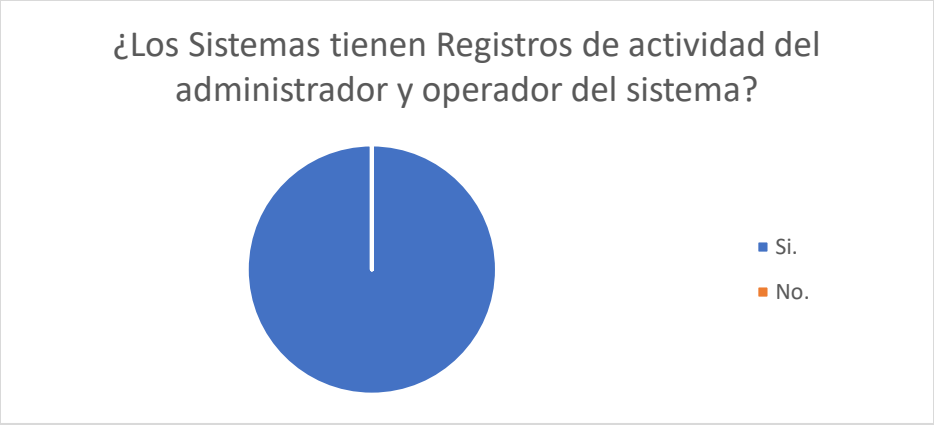
8. **¿Realizan separación de entornos de desarrollo, prueba y producción?**



Observación:

En el momento de desarrollo se realiza funciones códigos para los procesos respectivos para el funcionamiento del sistema, en el entorno de prueba se encuentran posibles bugs que se pueden corregir para que el sistema pueda ser instalado en producción.

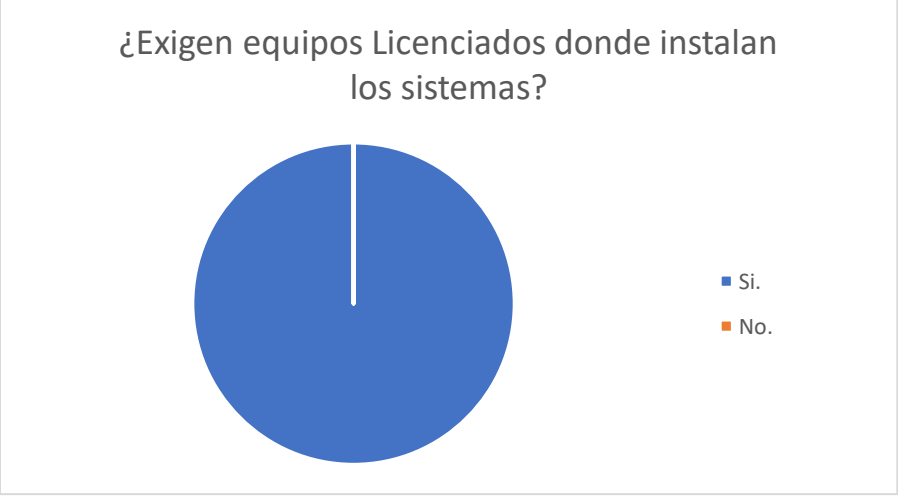
9. **¿Los Sistemas tienen Registros de actividad del administrador y operador del sistema?**



Observación:

Los Sistemas llevan un registro llamado huellas, Indica quien inicio sesión, hora y fecha además tienen un ambiente muy distinto del administrador y usuario no puede ser consultado ni verificado si no es por soporte de la empresa.

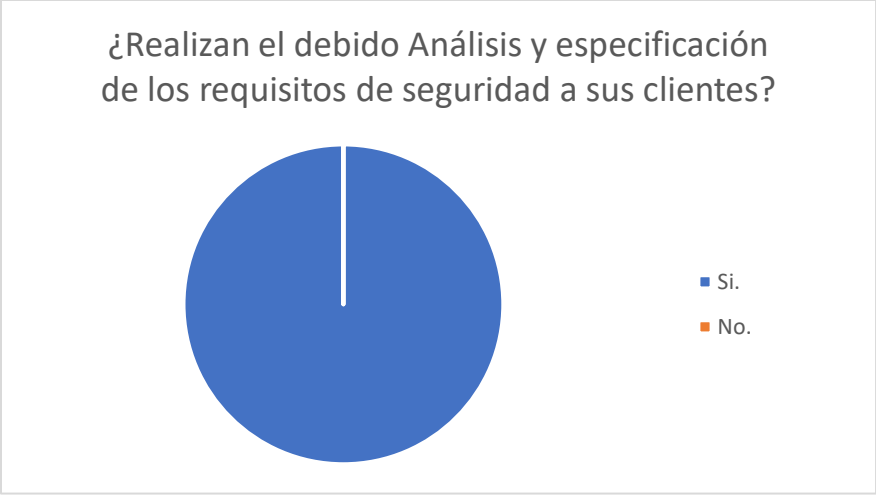
10. **¿Exigen equipos Licenciados donde instalan los sistemas?**



Observación:

Es un punto muy importante por políticas de seguridad ya que la misma empresa se encarga de licenciamiento de equipos para instalación de sistemas.

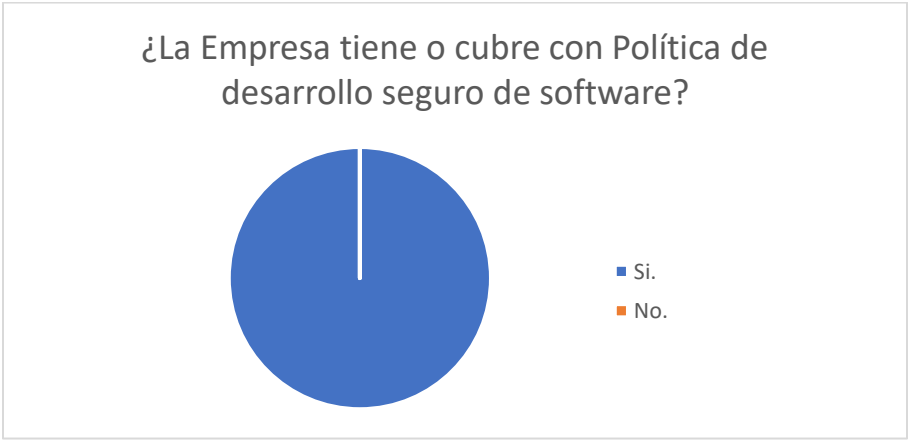
11. **¿Realizan el debido Análisis y especificación de los requisitos de seguridad a sus clientes?**



Observación:

Se le da una charla especificando puntos importantes de seguridad, licenciamiento, equipos necesarios y instalación del sistema.

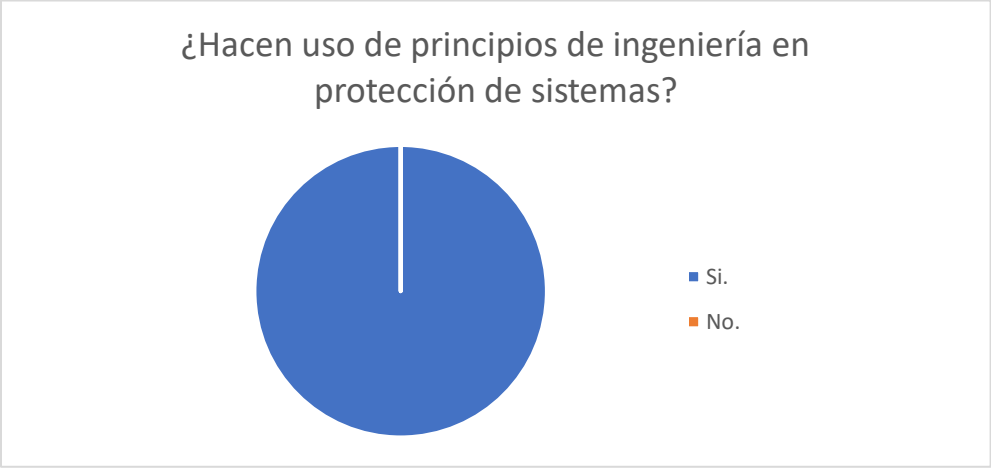
12. **¿La Empresa tiene o cubre con Política de desarrollo seguro de software?**



Observación:

Su nivel de encriptación de muy seguro además ellos brindan soporte y manteamientos por caídas del sistema.

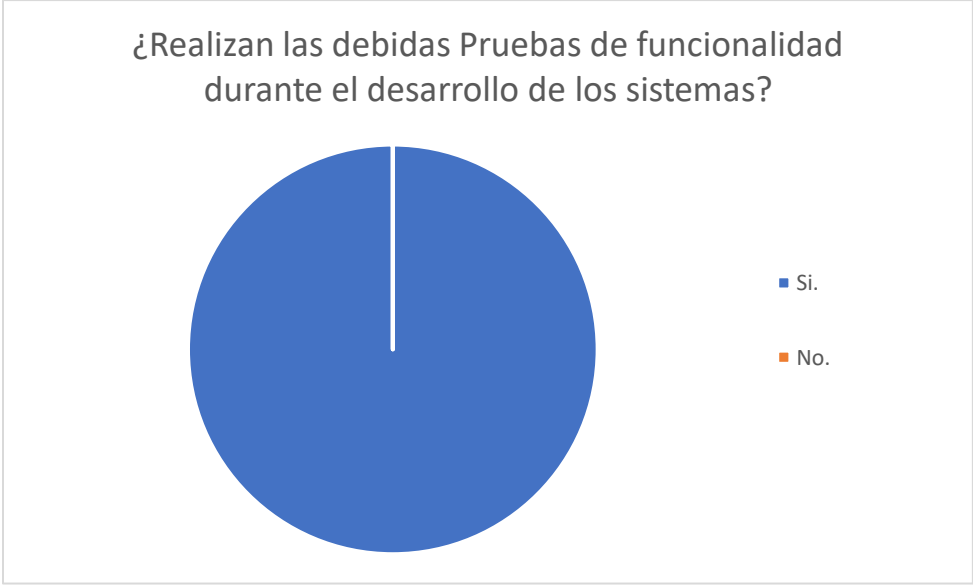
13. **¿Hacen uso de principios de ingeniería en protección de sistemas?**



Observación:

Los sistemas desarrollados en la empresa son íntegros confiables y disponibles para el correcto funcionamiento.

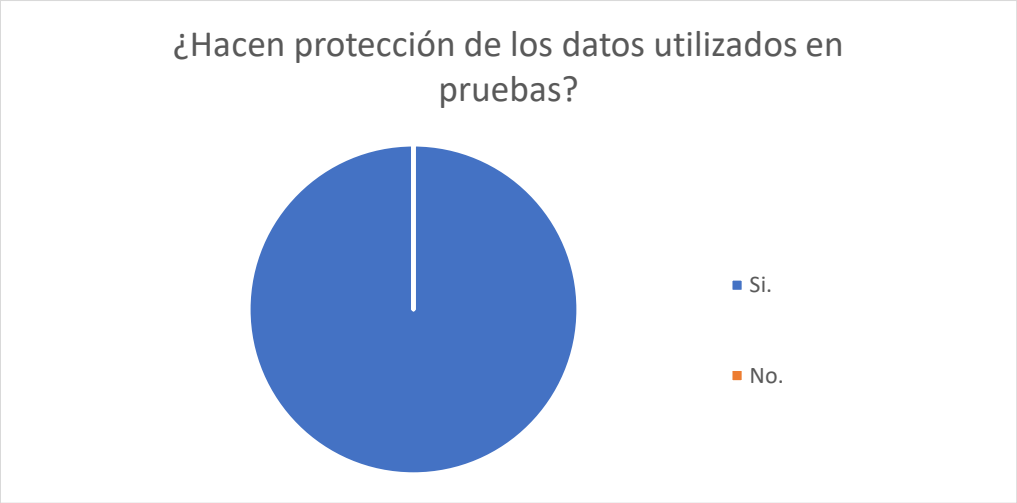
14. **¿Realizan las debidas Pruebas de funcionalidad durante el desarrollo de los sistemas?**



Observación:

Se realizan los procesos adecuados según el lineamiento de caja negra y caja blanca

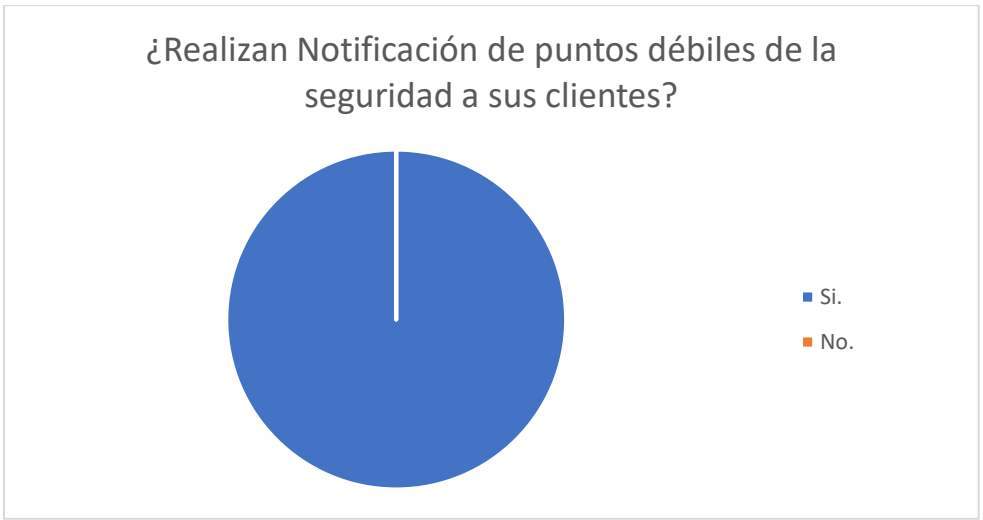
15. **¿Hacen protección de los datos utilizados en pruebas?**



Observación:

Los datos de prueba se encuentran dentro de la empresa.

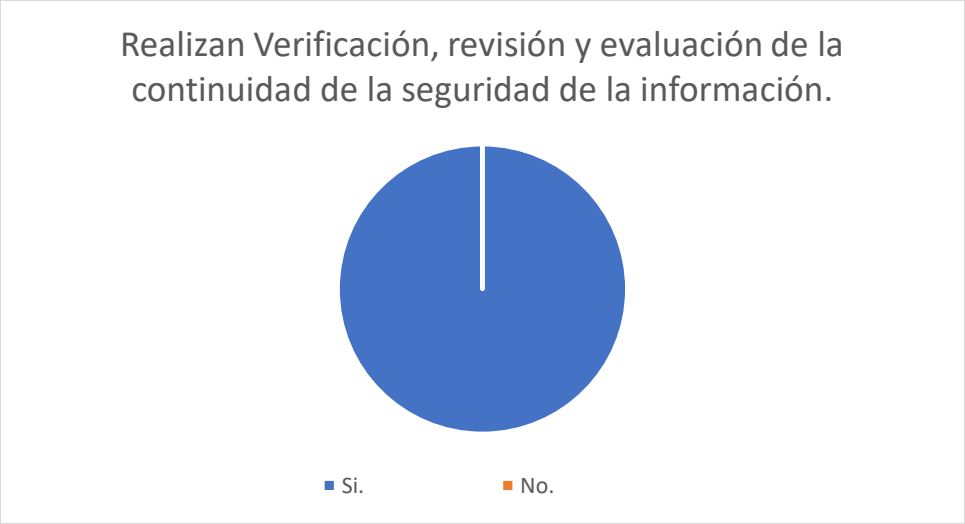
16. **¿Realizan Notificación de puntos débiles de la seguridad a sus clientes?**



Observación:

Cuando se encuentras puntos débiles o posibles errores o problema se le indica el procedimiento para solucionarlo y que el sistema trabaje correctamente.

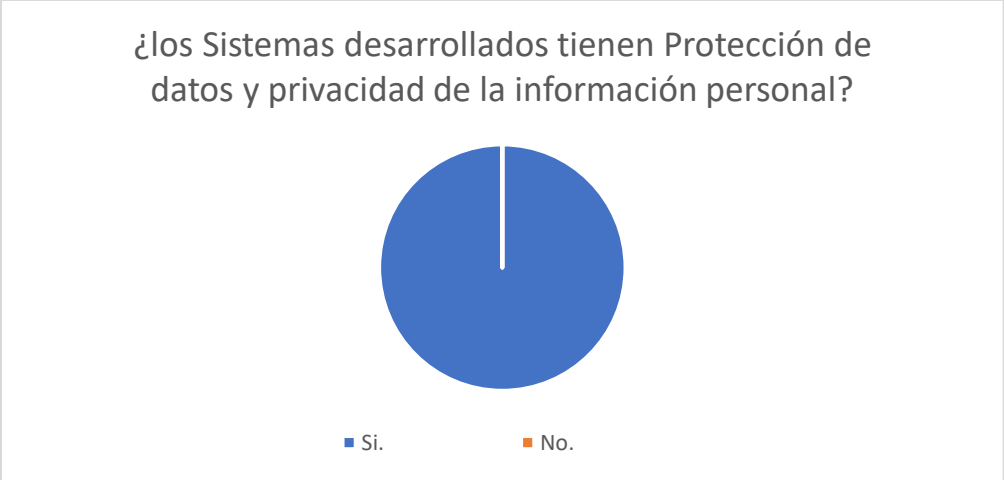
17. **Realizan Verificación, revisión y evaluación de la continuidad de la seguridad de la información.**



Observación:

En el momento de prueba se verifica y se revisa las posibles fallas de seguridad para evitar perdida de información

18. **¿los Sistemas desarrollados tienen Protección de datos y privacidad de la información personal?**



Observación:

Cada usuario utiliza un usuario diferente para el manejo del sistema.

19. ¿Protección de regulación de los controles criptográficos?

Observación:

En los sistemas se evidencia que se esta utilizando los controles de encriptación en el inicio de sesión.

20. ¿Cumple con los Requisitos de Gestión Corporativa?

Observación:

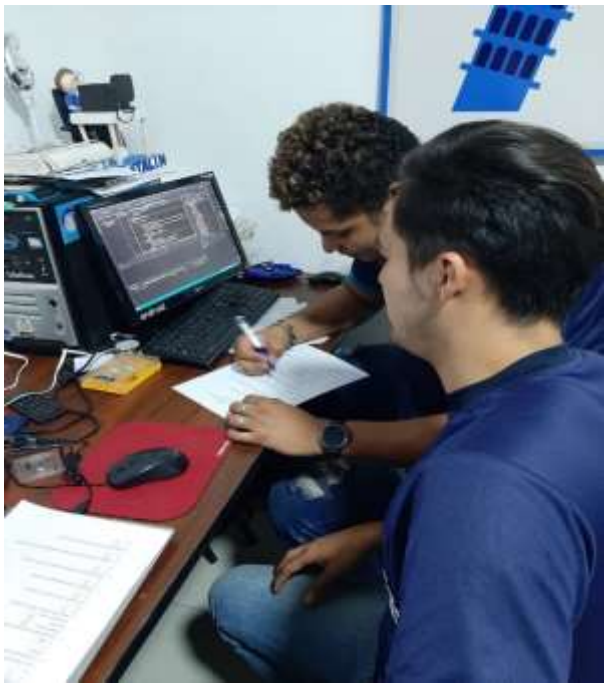
Si ya que especifica las condiciones de uso y políticas de seguridad al momento de negociación de algún sistema.

En resumen:

Estos términos de uso (el "acuerdo") se aplican al uso del Software Conto en cualquier plataforma o dispositivo, incluida cualquier función dentro del Software Conto como "NeoReply", "NeoTrust", "Next" y "NeoPass" (En conjunto el "Software Conto"). El acuerdo es un contrato legalmente vinculante entre Moss Solutions ("nosotros" o "nuestro" y cualquier persona ("usted" o "su") que acceda o use el Software Conto y cualquiera de sus funciones. Por favor revisa este acuerdo cuidadosamente antes de utilizar el Software Conto. Los términos de licencia también se aplican a cualquier servicio y actualización de Moss Solutions para el Software Conto, excepto en la medida que tengan términos diferentes. El Software Conto se ofrece sujeto a su aceptación de este acuerdo sin modificaciones. Al acceder o utilizar el Software Conto, usted acepta todos los términos y condiciones de este acuerdo como tales. Si adquiere una licencia válida con Id. Licencia para el software, se aplicarán los siguientes términos. No podrá compartir la Id. Licencia o las credenciales de acceso.

FOTOS

Evaluación al Codificador de los Sistemas



Evaluación al Diseñador y Gerente de la Empresa