UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIOS DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Gestión de seguridad de la información basada en la Norma ISO/IEC 27001 dirigido para la empresa Redondos S.A., Huacho

Tesis para obtener el título profesional de Ingeniero en informática y de sistemas

Autor

Montoya Mansilla, Nilton César.

Asesor

Ascón Valdivia, Oscar

Código ORCID: 0000-0003-3899-7259

CHIMBOTE – PERÚ

2021

Palabras Clave

Tema	**Seguridad de la Información**
Especialidad	Gestión

Keywords

Topic	**Security of the information**
Specialty	**Management**

Línea de Investigación

Línea	Sistema de gestión
Área	Gestión
Sub Área	Economía y negocios
Disciplina	Negocios y management

Titulo

Gestión de seguridad de la información basada en la Norma ISO/IEC 27001 dirigido para la empresa Redondos S.A., Huacho

Resumen

En este trabajo se propuso diseñar un sistema de gestión de seguridad de la información basada en la norma ISO/IEC 27001 para un buen manejo del sistema de información en la empresa Redondos, S.A. respecto a lo investigativo es un estudio descriptivo, no experimental, se aplicó la Norma ISO/IEC 27001, para encontrar las debilidadesde la seguridad de datos, y luego valorar y proponer mejoras en los niveles de seguridad. Como resultado del estudio se logró mejoras en los niveles de seguridad, evitar de esta manera cualquier riesgo en la integridad de la información, ante posibles amenazas que se puedan presentar interna o externamente en el normal desarrollo de actividades de la institución.

Abstract

In this work, it was proposed to design an information security management system based on the ISO / IEC 27001 standard for a good management of the information system in the company Redondos, S.A. Regarding the investigative, it is a descriptive study, not experimental, the ISO / IEC 27001 Standard was applied, to find the weaknesses of data security, and then assess and propose improvements in the security levels. As a result of the study, improvements were achieved in security levels, thus avoiding any risk to the integrity of the information, in the face of possible threats that may arise internally or externally in the normal development of the institution's activities.

Índice

Palabras Clave i

Resumen iii

Abstract iv

1. Introducción 1

2. Metodología 11

3. Resultados 13

4. Análisis y discusión 47

5. Conclusiones y Recomendaciones 48

6. Referencias Bibliográficas 49

7. Anexos 51

1. Introducción

De los antecedentes encontrados se han abordado los trabajos más relevantes a esta investigación:

Barrantes y Hugo (2012), se propusieron reducir y mitigar la presencia de riesgos de los activos de la información mediante la implementación de un sistema de gestión de seguridad en procesos tecnológicos en la gerencia de tecnología de Card Perú, S.A. para el desarrollo utilizaron la guía PMBOK y en la gestión de los riesgos MAGERIT. Se evidencio que no se tiene políticas ni cultura para salvaguardar la información, causando un grave riesgo a los activos de la información. lo relevante obtenido de la aplicación del SGSS se refleja en el 78.5% en promedio, lográndose detectar de oportunamente casos de vulnerabilidad, posibilitando mitigar riesgos. Asimismo, se detectó que los activos de información no poseían los controles necesarios diseñados para tal fin, controles como: preventivos, correctivos y predictivo. Finalmente se incrementó la seguridad de los activos de la información, garantizando así detectar oportunamente los riesgos.

Alcantara (2015) diseño una guía para la implementación de seguridad utilizando la norma ISO/IEC 27001, aplicados a los sistemas de información de una comisaría. Se evidenció un incremento del nivel de la seguridad de las aplicaciones informáticas, así mismo se logró incrementar políticas de seguridad reflejándose en las buenas prácticas, que benefician positivamente a la institución permitiéndole la detección de anomalías enla seguridad de la información. Al aplicar el tratamiento de riesgos, incidió en ladisminución de niveles de riesgos con respecto a los activos de información, consideradosamenazas y vulnerabilidades en la institución, esto manifestado en un plan adecuado para abordarlos y tomar las precauciones necesarias que minimicen sus impactos.

Guzmán (2015) se propuso diseñar un Sistema para gestionar la seguridad de la información aplicando la norma NTC-ISO-IEC 27001:2013. Los resultados evidenciaronen los trabajadores no existe una cultura de seguridad, es decir poca concientización de larelevancia de la información y el rol dentro de las actividades que se desarrolla en la empresa IGM S.A., en ese aspecto la empresa está en nivel medio, por lo complejidad dela infraestructura tecnológica. Se ha demostrado que el control de la información es del 46%, lo cual implica un riesgo a cualquier modo de vulnerabilidad, en ese sentido es necesario sumar esfuerzos para alcanzar un buen nivel de seguridad con los controles pertinentes.

Olaza (2017), en su investigación determinó el efecto de integridad de la información implementando la norma NTP ISO/IEC 24001, con fines de evitar riesgos y vulnerabilidad de acceso a la información de los activos del Ministerio de Educación. Como resultado se obtuvo un promedio de 10.76 de accesos sin autorización y/o modificación de los datos. Asimismo, un 1.55 de acceso sin autorización. No obstante, se logró reducir 9.21 de accesos y/o cambios. En ese sentido, al aplicar la Norma Técnica se obtuvo un significativo efecto en de 182 casos de vulnerabilidad a 50 casos.

Nieves (2017) se propuso diseñar un sistema de gestión de seguridad de información (SGSI) aplicando la Norma ISO/IEC 27001:2013. Sustentados en información recabada de los empleados respecto a las funciones y seguridad, ni mecanismos para salvaguardar la integridad de la información, así como, su autenticidad. Se concluye que por medio de la aplicación fue posible obtener la integridad y continuidad de los servicios informáticos, asimismo los accesos confiables y pertinentes, con los mecanismos de seguridad que salvaguarda a la información.

La presente investigación se justifica socialmente por qué, beneficia a los trabajadoresy clientes de la empresa, la propuesta ayudará a que los procesos de negocio funcionen adecuadamente, convirtiéndose de esta manera en un proyecto de impacto social, la seguridad de la información representa: claves, disponibilidad, confiabilidad, integridad de información sensible para mantener los niveles de competitividad, alcanzar los objetivos empresariales y su consecuente beneficio económico.

Asimismo, el presente proyecto, se justifica científicamente porque involucra la aplicación de una serie de conocimientos en las diferentes áreas y disciplinas que aportana gestionar de seguridad de información que hoy forman parte de la vida misma en el desempeño profesional de cada persona, utilizando normas validadas por entornos ISO 27001, 27000 Por tanto, estos nuevos elementos de control al ser integrados van a formar parte de una nueva concepción de la seguridad en las empresas; la implementación de sistema de gestión de seguridad tiene el fin de proteger y mejorar la seguridad de los procesos a nivel físico y lógico de los activos basado en estándares internacionales comola serie 27000 que se apoya en controles de seguridad para minimizar el riesgo de posiblesataques y/o intrusiones en las redes, pérdida de información y otros, así como también definir un plan de acción para realizar los controles propuestos.

El problema operativo de la empresa Redondos S.A está vinculado a la deficiente seguridad de la información, general situaciones no favorables en tomar decisiones, en seaspecto se hace necesario una propuesta de seguridad de la información, para ello se toma como referencia la norma NTP ISO/IEC 27001:2013, a través del mismo, para detectar oportunamente todo riesgo que pueda presentarse a fin de tomar las medidas y controles para mitigarlos y no afecten a los activos, afrontarlo de manera documentada, sistemática,estructurada, repetible, eficiente. La ausencia del mismo presenta riesgos rutinarios, el cual puede ser visto desde un visón cualitativo y cuantitativo. Cualitativamente el deterioro no suele ser evolutivo y produce de forma directa la anulación de los documentos y de procedimientos, asimismo, genera una degradación de la productividad del activo como recurso o

interrupción de su funcionamiento de una forma más o menos profunda yduradera; cuantitativamente provoca pérdidas de valor económico ya que se introducen todos los costos de reposición de la funcionalidad, en las que se incluyen las reparaciones así como también las pérdidas económicas asociadas a la responsabilidad legal, es por ello que aporte del estudio se basa en implementar medidas que conlleven la preserva la integridad de la información. De lo anteriormente expuesto se formula el problema: ¿Cómo aplicar la norma ISO 27001: 2013 para el monitoreo y revisión de los sistemas de información en la empresa Redondos S.A.?

Para el desarrollo del estudio de aplicación de controles de la norma ISO 27001, es necesario conocimientos que fortalezcan la propuesta, por lo tanto, se ha conceptualizado y operacionalizado la variable de estudio.

ISO 27001

Es una norma que, aplicada en las empresas, útil para la buena gestión de la seguridad de la información en toda empresa para lograr una certificación bajo la normaISO 27001 (Kosutic, 2015). Pues hoy en día esta norma se ha convertido en valioso parapreservar la seguridad de la información, que ha sido tomada en una gran cantidad de empresas a nivel mundial.

Figura 1. Cantidad de certificaciones
Fuente: osutic 2015.

El ISO 27001 tiene como función cuidar la confidencialidad, así como la integridad ydisponibilidad de toda información que maneja una empresa. Indagando

los potenciales riesgos de vulnerabilidad a la información de las empresas, que tienen activos informáticos relevantes de gestión y toma de decisiones empresariales. Ante esta situaciónse trata de evitar que se presenten problemas para mitigar o tratar los riesgos (Kosutic, 2015). Por lo consiguiente esta norma está enfocada en gestionar los riesgos, desde su aparición para luego tratarlas, también en la confidencialidad, considerando las importancia y valor de la información, mantenerlas integras, a decir exactas y complitud.(Kosutic, 2015).

Figura 2: Función De La ISO 27001.

Fuente: Kosutic - 2015.

Según la ISO 27001 se tiene cuatro ventajas comerciales esenciales que puede alcanzaruna empresa, si se atreve a implementar la norma para salvaguardar sus activos informáticos: cumplir con los requerimientos legales, lograr ventajas comerciales, menoscostos y una buena organización, como lo describe Kosutic (2015): La ISO 27001 es unanorma perfecta para la seguridad de la información, se ajusta a las normas legales y requerimientos de protección de datos, privacidad y control de las Tecnologías deInformación en las empresas. Lo cierto es que la competitividad del mercado exige a las empresas tener mucho cuidado con la información que se administra para sus operacionescomerciales, sobre todo con el trato cauteloso a sus clientes en conservar las necesidadesy satisfacción. En ese aspecto la Norma ISO 27001 está diseñada para para evitar incidencias de seguridad de la información en diferente magnitud de riesgo, la perdida dela información es más costoso, sin embargo, muy poco se invierte en implementar sistemas bajo normas internacionales.

Figura 3. Gestión del Riesgo.
Fuente: Kosutic - 2015.

Los Dominios de Seguridad de la Información:

La ISO 27001 para su aplicación en los procesos organizativos empresariales proponeuna secuencia de Dominios Tecnológicos; construcción que requiere la participación de un equipo multidisciplinario que actúen con responsabilidad en cada dominio de la norma.(Kosutic, 2015). Los dominios que contempla la Norma ISO 27001: Dominio de Políticade Seguridad, establecidos en los requerimientos y políticas de la organización; Dominio Organización de la Seguridad de la Información: la empresa establece las políticas de seguridad, y el administrador del modelo para la coordinación y revisión del sistema; Dominio Gestión de Activos: se inventan los activos y un personal responsables del control; Dominio Seguridad de los Recursos Humanos: se establecen las medidas de seguridad para preservar la información y las buenas prácticas del personal de la organización. Dominio Seguridad física y del ambiente: proteger los equipos de hardwarey espacios físicos donde se encuentran los servidores o equipos que registran mediante barreras y controles de seguridad. Dominio Gestión de las comunicaciones y operaciones: establece los procedimientos y responsabilidades para una correcta ejecución de la información. Dominio Control de Acceso: establecer políticas con acceso autorizado a lainformación mediante procedimientos de control establecidos por la organización. Dominio Adquisición, desarrollo y mantenimiento de los sistemas de información: validopara el software que se desarrolla en la empresa o son adquiridos

por tercero para salvaguardar la seguridad de la información. Dominio Gestión de

incidentes en la seguridad de la información: aplicar mecanismos para gestionar las incidencias de posibles riesgos. Dominio Gestión de la Continuidad del Negocio: evitar la paralización de la operatividad de la empresa mediante un plan de continuidad. Dominio Cumplimiento: garantizar el cumplimiento de los requerimientos legales en las diferentesestas de la implementación de los sistemas de información.

Análisis de la empresa.

Descripción de la Empresa.

Redondos es una empresa relacionada al rublo de alimentos de productos avícolas,piscícolas y acuícolas siendo una empresa que mayor presencia comercial tiene en el Perú,imponiendo liderazgo en la cadena de producción y comercialización de productos avícolas,La empresa empresarialmente tiene una trayectoria de 45 años comercializando productos alimenticios. A lo largo de los años fue creciendo e incrementando personal en las diferentes áreas de producción y unidades administrativas en la provincia de Huaura y Huaral. Redondos S.A esta comprometido en la comercialización de productos cárnicos caracterizados por ser nutritivos y de excelente calidad en el bienestar de las familias.

Visión. Ser la empresa líder en el mercado de productos cárnicos, innovando y agregandovalor a nuestros clientes y consumidores a nivel nación, con proyección internacional

Misión. Generar desarrollo en el país. Contribuyendo con la alimentación, generandotrabajo y bienestar.

Pirámide de la bioseguridad.

En la figura 4 se muestra una pirámide de vital importancia para la organización que son tomadas a medidas sanitarias, reducir el ingreso de microrganismos externos a las diversas plantas y granjas.

Figura 4. Pirámide de sanidad Redondos S.A.

Son aplicadas de las siguientes medidas:

Los movimientos de los personales entre pollos y pavos y cerdos en mismo nivel dela pirámide sanitaria, es de vital importancia tomadas con el área de sanidad. Así mismo son consideradas con las visitas externas que son coordinadas con cincodías de anticipación. Además, la pirámide de sanidad asegura una producción cárnica de calidad.

Organigrama tecnología de la información.

En la figura 5 se presenta la jerarquía del área de tecnologías de información, cumpliendo el resguardo y seguridad de activos de la Información, además es supervisadopor los coordinadores y jefe del área. Este equipo cumple las funciones de Soporte, Inventario, Desarrollo, backup de usuarios, servidores y base de datos de la organización.

Figura 5. Tecnología de la información.

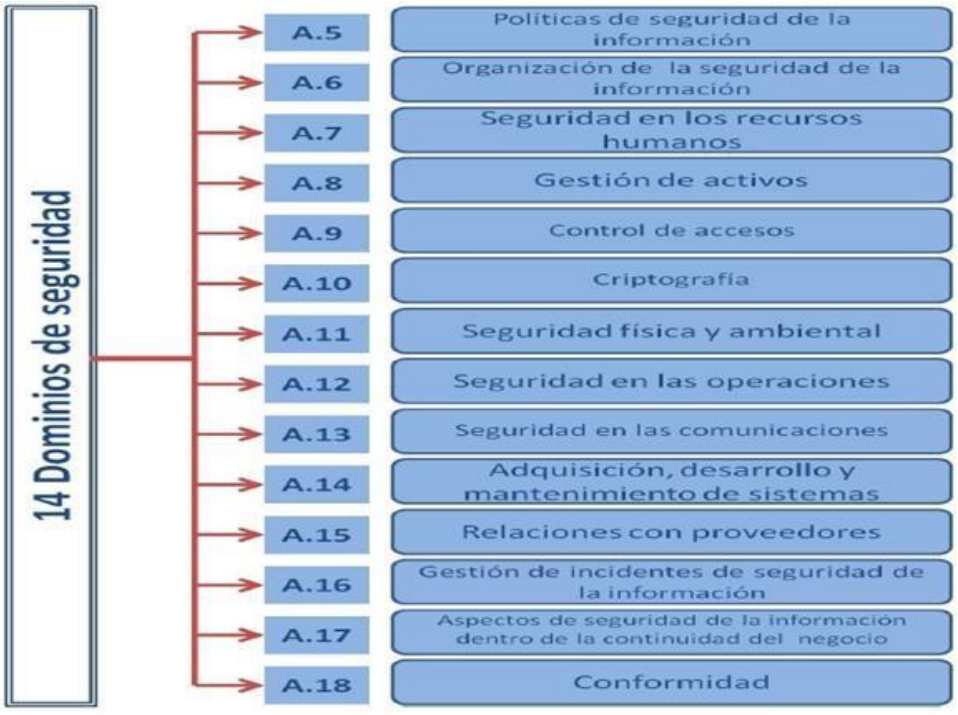

Figura 6: Dominios de la ISO 27001:2013
Fuente: ISO 27001:2013.

En vista que la investigación tiene un alcance de carácter descriptivo, no es posible plantearuna hipótesis debido a que no se intenta correlacionar o explicar casualidad de variables, y el objetivo a alcanzar está claro. Por tal razón se considera una Hipótesis Implícita.

Los objetivos planteados para la siguiente investigación fueron, como objetivo general: Aplicar la norma ISO 27001 para el monitoreo y revisión de los sistemas de información en la empresa Redondos S.A; y, los objetivos específicos: a) Identificar los riesgos en los sistemas de información de la empresa Redondos, S.A.; b) valorar los riesgos para minimizar las deficiencias a los que se encuentran sometido el sistema de información en la empresa Redondos, S.A, y c) establecer los procedimientos y controles para un mejor monitoreo y revisión del sistema de información en base a los criterios de la norma ISO 27001.

2. Metodología

Para fines de la presente investigación, la misma será del tipo descriptiva. que comprende la descripción, registro, análisis e interpretación de la naturaleza actual, y lacomposición o procesos de los fenómenos El enfoque se hará sobre conclusiones dominantes o sobre como el elemento estudiado se conduce o funciona en la actualidad.

Asimismo, se trata de un diseño no experimental, porque se manipuló ninguna variable; de corte transversal; porque los datos fueron tomados en un determinado momento de la investigación. Se basó fundamentalmente en la observación de los fenómenos estudiados tal y como se dieron en su contexto natural analizándolos y procesándolos.

Las técnicas e instrumentos de recolección de datos utilizados fueron: La técnica de la observación, la cual consistió en visualizar o captar mediante la vista, en forma sistemática,cualquier hecho, fenómeno o situación que se produzca en la naturaleza o en la sociedad, en función de los objetivos de investigación preestablecidos. En el caso de la observación libre o no estructurada, la cual se utilizó en la presente investigación se emplearon instrumentos tales como: diario de campo, libreta o cuaderno de notas, cámara fotográfica, entre otros, a su vez se hizo una lista de cotejo en la cual se indicó la presencia o ausencia de los diferentes aspectos a ser observados.

La encuesta, la cual es una técnica que permitió obtener información que suministró la muestra, fue aplicado a 40 trabajadores del área de informática, quienes salvaguardan la información de la empresa, El instrumento manejado se realizó de forma escrita mediante un formato en papelcontentivo con una serie de preguntas, el cual fue llenado por el encuestado, sin intervencióndel encuestador, el mismo que estuvo estructurado con preguntas cerradas.

El trabajo de investigación estuvo basado gestionar de forma correcta la seguridad de la información basada en la Norma Internacional ISO 27001:2013, la cual se presentaron los siguientes alcances:

Diseño metodológico de la norma ISO 27001:2013. Se aplicó esta norma para implantar un sistema de gestión de seguridad de la información (SGSI), importante a considerar como eje primordial, para los casos de evaluación de riesgos. Como bien estáestablecido en Isotool que comprende las siguientes fases:

- Identificación de los Activos de Información y sus responsables, del soporte físico ylas informaciones que se maneja en la organización
- Identificación de las Vulnerabilidades de cada activo: detectar cuales son las aquellas debilidades inherentes al activo haciendo vulnerable a riesgos a la integridad de la información.
- Identificación de amenazas: que puedan presentarse y causar perjuicios en los activosinformáticos de la organización físicamente o a través de internet.
- Identificación de los requisitos legales y contractuales que involucra a todo el actor dela cadena de producción de la empresa.
- Identificación de los riesgos: clasificar los activos y las probables amenazas o vulnerabilidades que causen daño a los activos empresariales, relacionados con las disponibilidad, confidencialidad e integridad de los activos de información.
- Cálculo del riesgo: partiendo de la probable presencia del riesgo e impacto que generarsobre la organización.
- Plan de tratamiento del riesgo: definición de políticas en el tratamiento de riesgos, seleccionando las medidas de control para cada riesgo. En ese sentido, el SGSI no permite establecer políticas y procedimientos vinculados a los objetivos planificados en una organización. A fin de mantener un nivel de seguridad respecto a los riesgos y vulnerabilidades que debe asumir la organización. (Aguilera, 2015).

Metodología Magerit. Permite analizar el impacto ante una posible vulneración en la seguridad de la información,identificando y gestionado los riesgos ante las amenazas que puedan surgir para ser identificados oportunamente y aplicar las medidas correctivas. En ese aspecto se enfoca a ubicar, analizar los riesgos más críticos a la seguridad de los sistemas de información. En ese sentido, está alineado con los estándares de ISO. (Gutiérrez, 2015).

3. Resultados

Para la identificación de los riesgos de la empresa se aplicó un cuestionario aplicado al personal de la Empresa Redondos, S.A. El instrumento construido constó de un total de treinta y tres ítems, formuladas en basea los catorce dominios establecidos en la norma ISO/IEC 27001, estos ayudaron al estudio de la seguridad de la información, el mismo fue aplicado al total de la muestra seleccionada,la cual estuvo representada por cuarenta empleados de la empresa Redondos, S.A., los resultados se muestran a continuación:

Variable: Seguridad de la información.

Dominio: Política de seguridad de la información.

Estuvo comprendida de dos ítems que permitieron la obtención de información con la finalidad de conocer si en la empresa Redondos, S.A, se tiene soporte de seguridad de la información según los lineamientos establecidos en la norma ISO/IEC 27001.

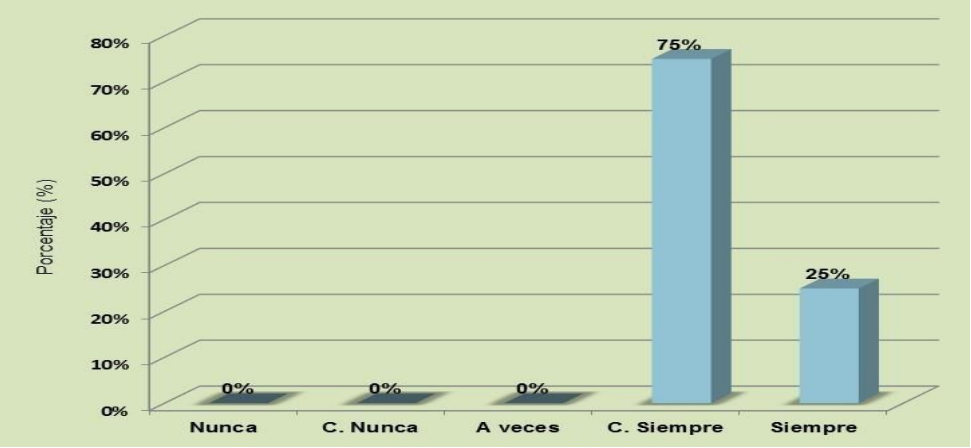

Figura 7. preocupación por parte de la dirección de la empresa Redondos, S.A., en elaborar documentossobre las políticas de seguridad a los activos de información, procedimientos a seguir a los riesgos a los que está sometida la información.

De acuerdo al resultado obtenido y representado en la figura anterior en base a cada unode los márgenes de respuestas, el 75% de los entrevistados afirman que casi siempre existe una preocupación por parte de la dirección de la empresa

Redondos, S.A., en establecer las políticas para la seguridad de los activos, siendo estas aprobadas por la gerencia de la empresa,y su correspondiente publicación interna y externamente.

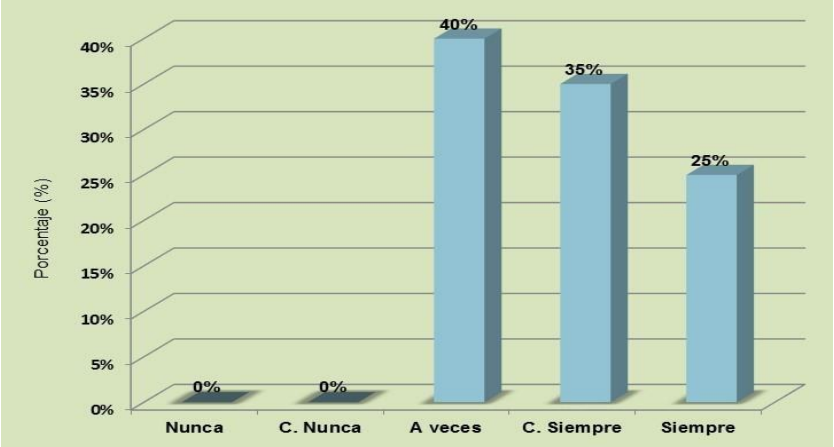

Figura 8. Mecanismos que los ayuden a tomar acciones rápidas y correctivas al peligro de lainformación.

El 40% de los entrevistados manifiestan en base al criterio de respuestas que a veces se cuentan con mecanismos que los ayudan a tomar acciones rápidas y de forma correctivas. Así mismo el 35% y el 25% opinan que casi siempre o siempre respectivamente cuentan con dichos mecanismos. Estos ayudan a tomar acciones correctivas rápidas cuando los sistemas de información se encuentran en peligro, siendo este un factor imprescindible para lograr una eficaz gestión de seguridad y así tener un conocimiento de todo lo que se necesita para realizartal evaluación, incluyendo tanto la forma como el momento en que hacerlo al momento de presentarse algún imprevisto.

Dominio: Organización de seguridad de la información.

Se estudió se enfocó a la formulación de tres ítems que permitieron la obtención de la información en como: acceso, procesamiento, comunicación y gestión de la seguridad de la información en la empresa Redondos, S.A., en base a criterios de la norma ISO/IEC 27001.

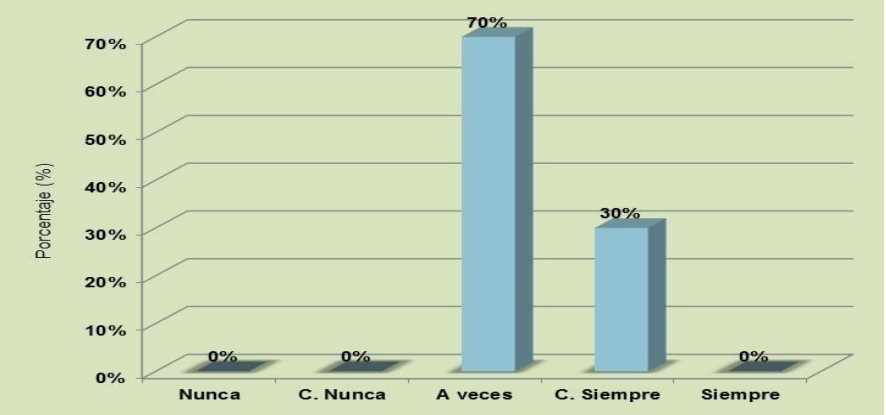

Figura 9. La junta directiva y los jefes de los distintos departamentos de la empresa Redondos, S.A., entienden, apoyan y llevan de forma eficaz las políticas de seguridad internamente en la empresa.

Un 70% de los entrevistados afirman como a veces y el restante 30% como casi siempre el apoyo que brinda la junta directiva de la empresa Redondos, S.A., cumplen cada una de las políticas establecidas para la seguridad de la información, definiendo y asignando de mejor manera los roles y responsabilidades, que ayudan a reducir la presencia de alguna amenaza quegenere alguna actualización sin autorización o no intencional o mal uso de los activos que se tiene en la empresa.

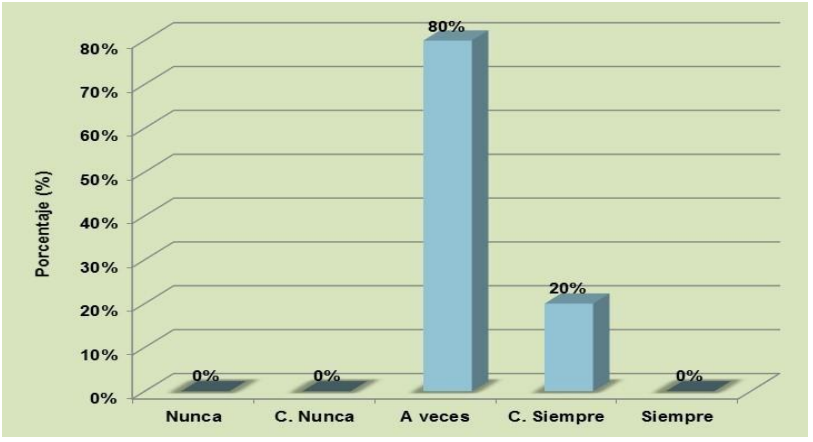

Figura 10. La junta directiva y los demás implicados se preocupan de que el resto del personal se concientice conla importancia de la seguridad de la información, las responsabilidades que cada uno tiene dentro de este tema.

El 80% de los empleados que fueron entrevistados afirmaron que a veces y el restante 20% como casi siempre la junta directiva de la empresa Redondos, S.A., muestra preocupación en que su personal genere concientización de la importancia de la seguridad de la información, ayudan a generar una cultura informática y condiciones necesarias en los sistemas de información a lograr objetivos para los que fueron diseñados.

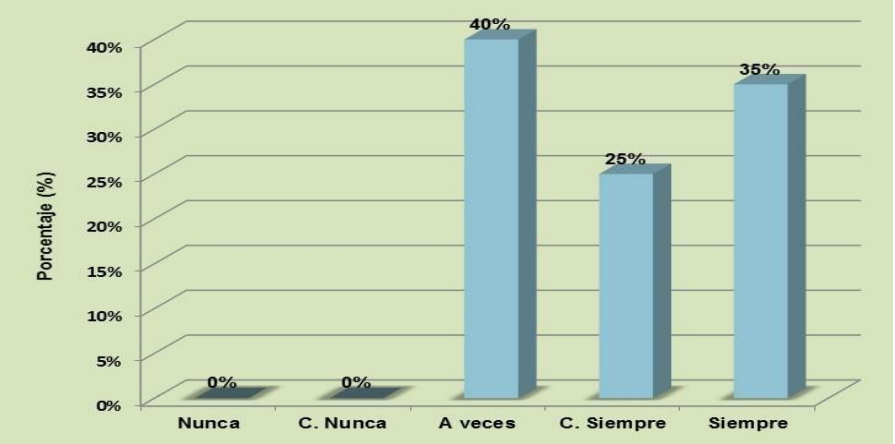

Figura 11. Procesos definidos e implementados para la autorización de recursos de procesamiento de la información.

El 40% de los empleados entrevistados determinó que a veces se definen e implementan en la empresa Redondos, S.A. diferentes procesos que generan la autorización de recursos de procesamiento de la información por la junta directiva, en base a esto se ve la importancia que esta guarda en el proceso de planificación y coordinación relacionados con el manejo de la información, generando un gran ahorro de estos recursos ya que ayudan a facilitar las labores de los usuarios a la hora de acceder a la información, mientras que el 25% y el 35% siempre y casi siempre respectivamente.

Dominio: Seguridad de los recursos humanos

Esta tiene como finalidad asegurar en los empleados y contratistas entiendan sus responsabilidades y la conveniencia en los roles desigandos, la misma se estudió a través de laaplicación de un total de 3 ítems.

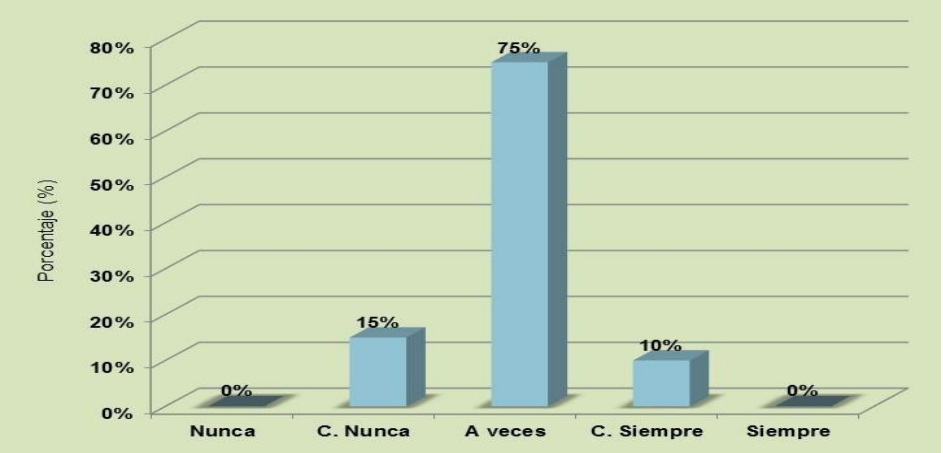

Figura 12. Mecanismos de verificación de los antecedentes de candidatos que ocupan o buscana ocupar un cargo dentro de la empresa.

El 75% de los empleados entrevistados mostraron a veces, el 15% como casi nunca y el restante 10% casi siempre se cuentan con los mecanismos para realizar los procesos de verificación de los antecedentes de cada uno de los candidatos que ocupan o buscan a ocupar funciones dentro de la organización, siendo este un factor en el que debe centrar mucha atención por la importancia que este tiene ya que les permite asegurarse de que sus procesos de contrataciones sean los más ideales y se apliquen de forma eficiente, de igual forma el postulante tendrá los antecedentes y la experiencia de forma argumentada y de esta forma podrá desempeñar a la perfección los requerimientos de la vacante.

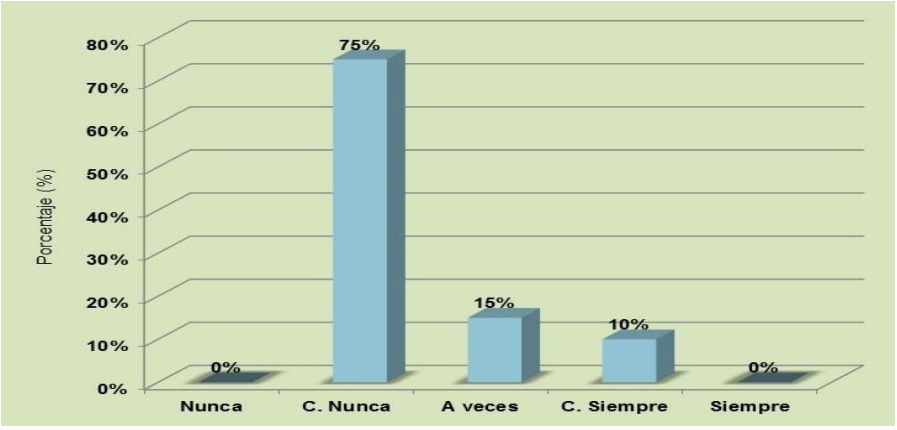

Figura 13. Aplicación de procesos disciplinarios por infringir las normas de seguridad deinformación.

El 75% de los empleados afirmaron que casi nunca se aplican procesos disciplinarios por infracción a las normas no se cumplen o vulnerados por los usuarios, mientras que el 15% manifestó que a veces y el 10% casi siempre, es sugerible que la gerencia tome acciones para un correcto comportamiento de los empleados. Es decir, cumplir las reglas internas establecidas con antelación, de ser necesario aplicar estas de forma preventiva, correctiva y progresiva.

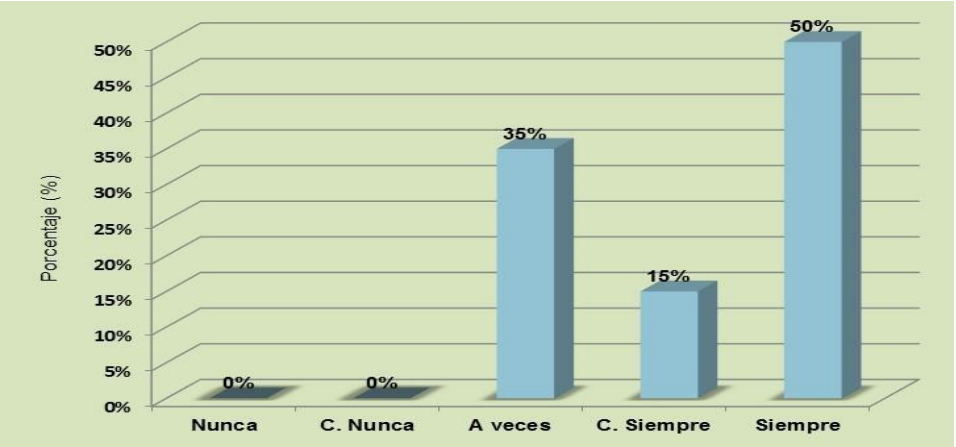

Figura 14. Cancelación de acceso de los empleados, contratistas o usuarios de la información y losrecursos una vez terminado su empleo, contrato o acuerdo dentro de la empresa.

El 50% de los empleados manifestaron que siempre, el 15 % casi siempre y el 35% a veces se encuentran establecidos los procedimientos para realizar el retiro de los derechos de acceso de la información y los recursos una vez terminado su empleo, contrato o acuerdo dentro de la empresa.

Dominio: Gestión de activos.

Esta busca a identifica con que activos cuenta la organización y cuáles son los roles y responsabilidades apropiados que deben darse.

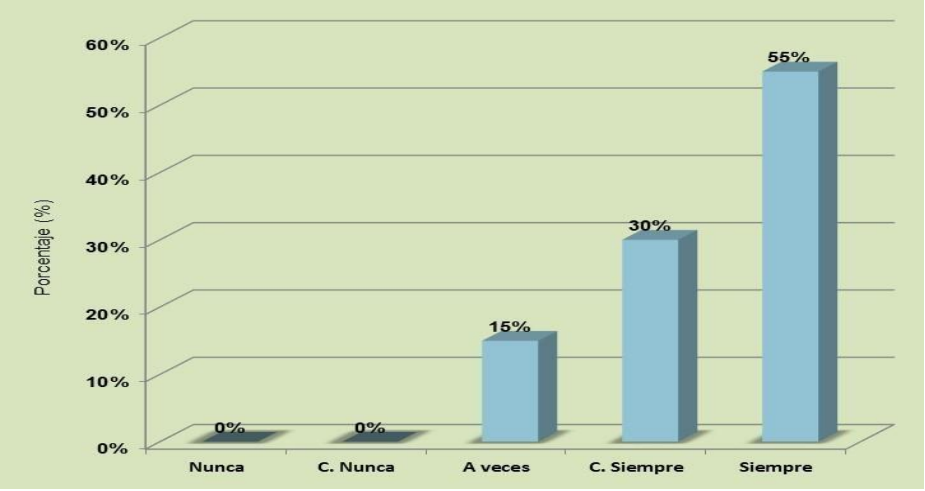

Figura 15. Mecanismos de identificación de cada uno de los activos utilizados en la empresaRedondos, S.A., que contengan informaciones del usuario.

El 55% de los entrevistados manifestaron como siempre, el 30% casi siempre y el restante 15% a veces se cuentan con mecanismos en la empresa Redondos, S.A., para la identificación de cada uno de sus activos fijos, ya que estos buscan a proporcionar información al momento de tomar decisiones y tener un mejor manejo de inventario, además de brindar la transparenciaque se necesita a otras partes interesadas sobre el funcionamiento de la empresa, tales como auditores internos e independientes.

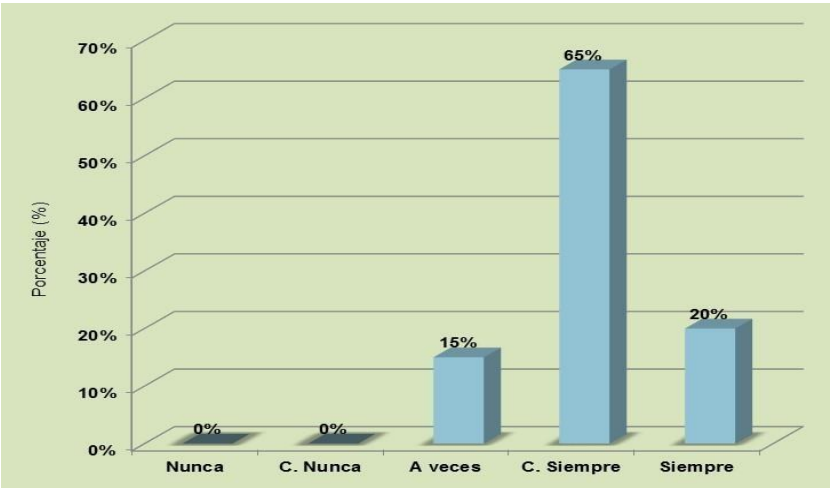

Figura 16. Inventarios de equipos informáticos y de comunicación.

Un 65% del personal entrevistado hizo ver que los procesos de inventarios casi siempre se realizan, el 20% siempre y el 15% casi nunca, dando evidencia que estos generan

una mayor facilidad a la hora de informar a la dirección o a los clientes la disponibilidad de los activos que se tiene que ayudan que las asignaciones diarias se puedan cumplir de forma efectiva y eficaz.

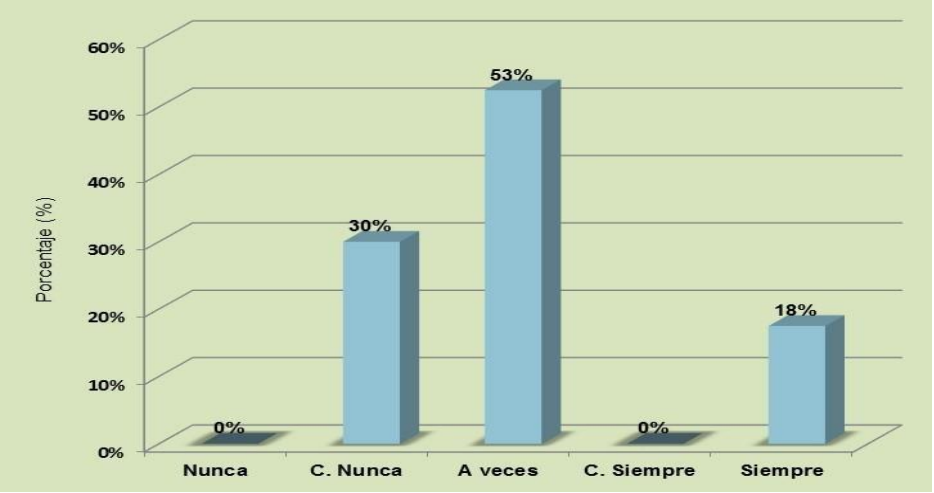

Figura 17. Directrices de clasificación de información: valor, requisitos legales, sensibilidad y criticidad.

El 53% de los empleados expresaron que a veces, el 30% casi nunca y el restante 18% siempre se generan directrices por parte de la organización para clasificar la información de acuerdo a su valor, lo que hace evidente que la misma tiene mucha deficiencia en base a estos criterios indispensables para la continuidad de sus procesos, ya que al tener una mejor clasificación se pueden generar indicativos asociados a el grado de necesidad, prioridad y de

protección con la que debe constar, a su vez comprender que existen diferentes elementos deinformación que necesitan un nivel más elevado de protección.

Dominio: Control de accesos

La finalidad es limitar el acceso a la información y las instalaciones de procesamiento dela información.

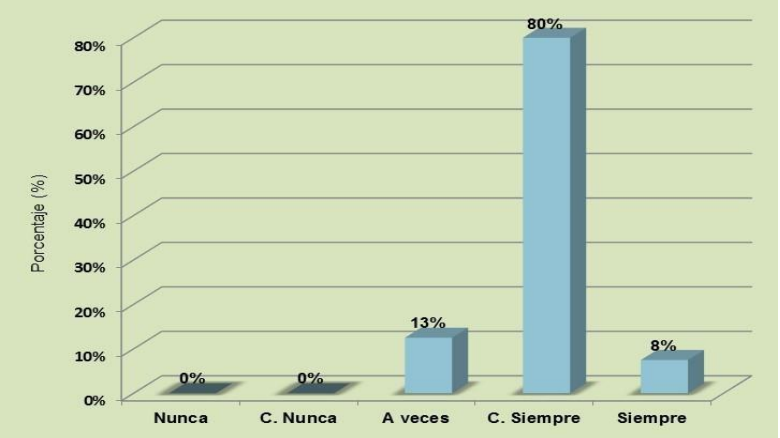

Figura 18. Procedimientos formales de registros de acceso al usuario.

El 80% de los entrevistados afirmaron que casi siempre y 13% que a veces existen procedimientos en la empresa Redondos S.A., asignar y cancelar el acceso a los sistemas yasí como también a los servicios de información, quedando evidenciado el compromiso en evaluar la eficiencia de la organización y participación de cada miembro de su empresa.

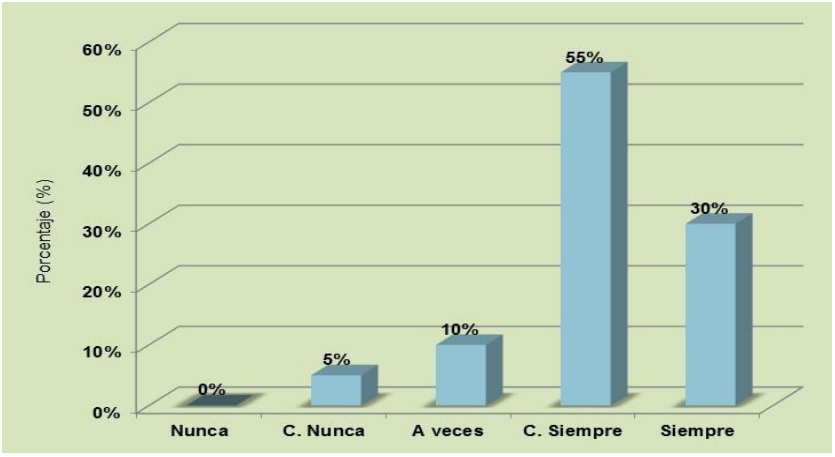

Figura 19. Control de contraseñas de usuarios para prevenir acceso no autorizadoa los sistemas de información.

El 55% expresó que casi siempre, el 30% siempre, 10% a veces y el restante 5% casi nuncase controlan los procesos para la asignación de contraseñas de usuarios, afirmándose que estosse encuentran bien definidos en cada una de sus bases con acceso a los servicios de red autorizaos

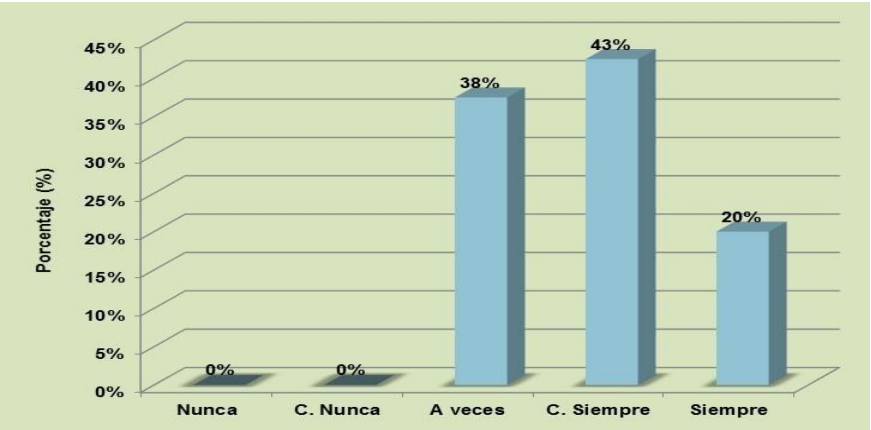

Figura 20. Mecanismos que motiven al personal a las buenas prácticas de acceso.

El 43% de los empleados entrevistados afirmaron que casi siempre, así como el 38% a veces, dicen que existen mecanismos en la empresa Redondos, S.A., motivador al personal a en las buenas prácticas para la elegir contraseñas, quedando claro el compromiso por parte de la organización de que la información que se maneja forme parte de uno de sus activos más valiosos y que se cuenten con canales eficientes para recuperar la información cuando esta se encuentre en peligro y que todas las operaciones se sigan llevando con total normalidad.

Dominio: Criptografía.

Esta busca asegurar el apropiado uso de la criptografía a fin de proteger la confidencialidad, autenticidad e integridad de la información.

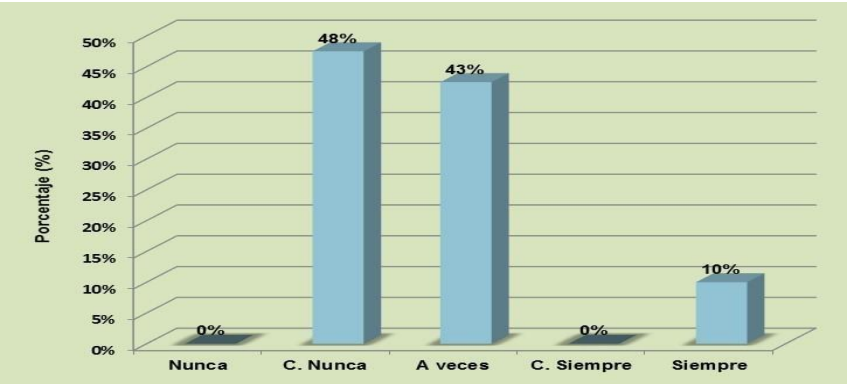

Figura 21. Medios criptográficos que buscan la protección de la confidencialidad, autenticidad o integridad de la información en la empresa.

El 45% de los entrevistados afirmaron que casi nunca, así como el 43% a veces dice quese cuentan con medios criptográficos en la empresa Redondos, S.A. que busquen la protecciónla confidencialidad, autenticidad o integridad de la información, quedando evidenciado que la empresa no conoce la importancia que esta tiene de los sistemas de información.

Dominio: Seguridad física y del entorno.

Esta busca impedir a los ambientes físicos a personas no autorizados, algún daño o interferencia a la información, así mismo, las instalaciones del centro de procesamiento de información de la organización.

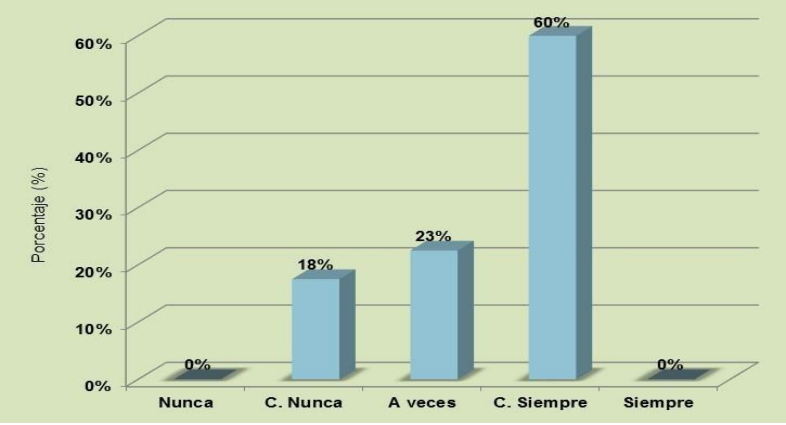

Figura 22. Parámetros de seguridad en las áreas con informacióne instalaciones de procesamiento de información.

El 60% de los empleados afirmaron que casi siempre se establecen de forma adecuada los parámetros de seguridad en la empresa Redondos, S.A., para cada una de las áreas que manejan información relacionada a cada una de sus operaciones, quedando de forma evidente que estas no son procesadas y manejadas de forma eficiente.

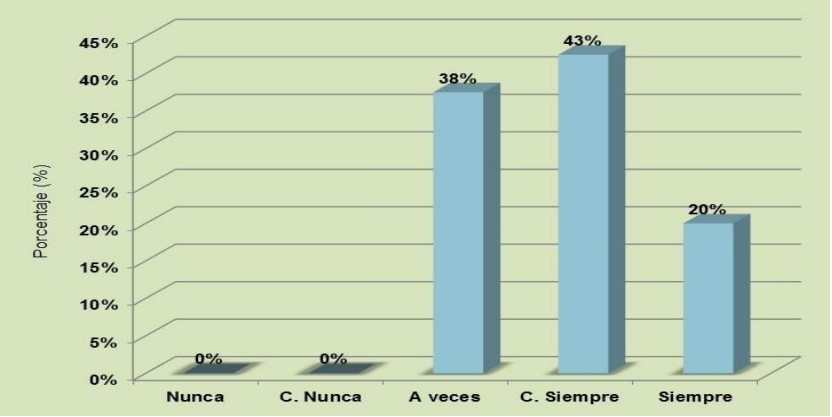

Figura 23. Aplicación de controles a las áreas de seguridadcon acceso sólo a personal autorizado.

Del total de empleados entrevistados catalogaron que a veces, casi siempre y siempre con un margen porcentual de 38, 43 y 20% respectivamente, son los mecanismos diseñados y se aplican cada uno de los controles de entrada utilizados para accesar a las áreas de seguridad,lo que hace evidente el compromiso por parte de la organización de mantener estos y así contar con un excelente registro de entradas y salidas del personal autorizado, de manera que se puedan registrar horarios y conocer qué tipo de operaciones han realizado y así contar con registros que los ayuden en un futuro a poder detectar y sustentar a través de evidencias cualquier anomalía que haya puesto en peligro algunos de sus activos de información.

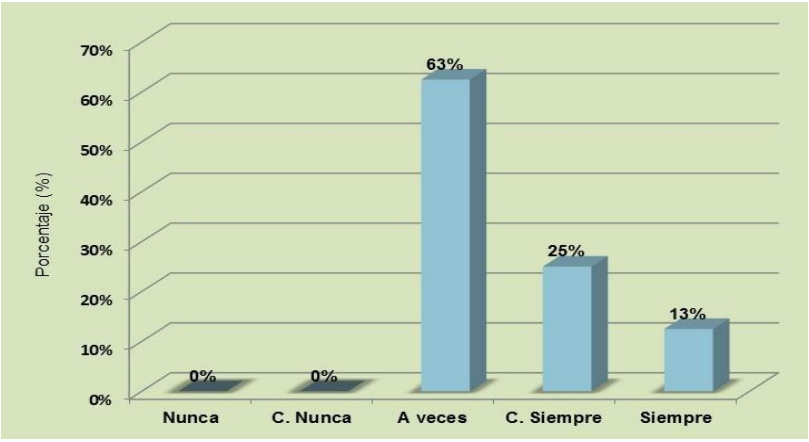

Figura 24. Controles de ingreso a las oficinas fuera del horario de trabajo.

El 63% de los entrevistados afirman que a veces, el 25% casi siempre y el restante 13% siempre la empresa lleva a cabo medianamente políticas de control de ingreso a las oficinas fuera del horario de trabajo, por lo que es necesario centrar y fortalecer ya que a pesar de que no se encuentre la totalidad del personal que labora frecuentemente igualmente se está haciendo uso de los activos de la información y los mismos quedan sometidos a múltiples amenazas.

Dominio: Seguridad en las operaciones

Esta busca asegurar el correcto procesamiento de la información con operatividad de sus instalaciones informáticas.

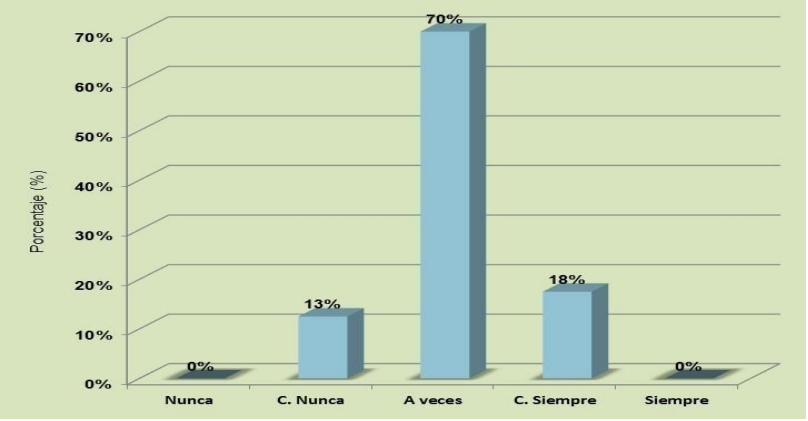

Figura 25. procedimientos operativos disponibles a los usuarios.

El 70% de los entrevistados declararon que a veces se dispone de procedimientos operativos a los usuarios, a pesar de los pocos con que se cuentan estos no son llevados de forma eficiente, es por ello es necesario el fortalecimiento que permitirá a la gerencia general aplicar indicadores de gestión a fin de medir el desempeño de sus operaciones y sus responsables.

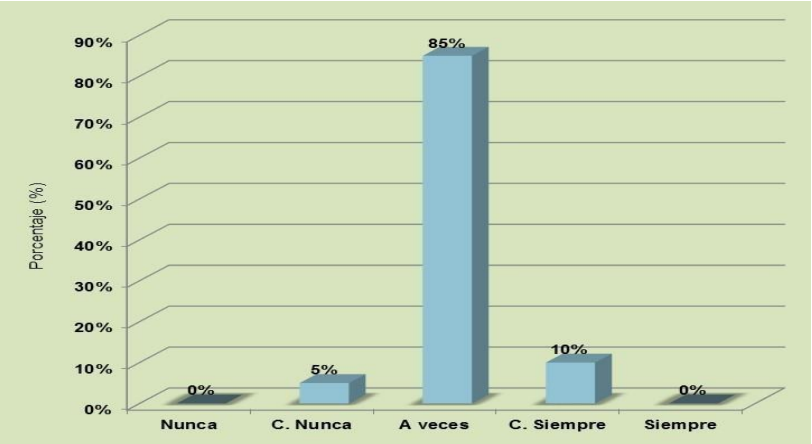

Figura 26. Control de cambios en los recursos y sistemas de procesamiento de la información

El 85% de los entrevistados afirman que a veces se controlan los cambios en los recursosy sistemas de procesamiento de información, mientras el restante 10% casi siempre, a pesarde esto se requiere que la organización cree una cultura que ayude a comprender los cambios en los procesos de negocio, instalaciones de procesamiento de la información y sistemas.

Dominio: Seguridad en las comunicaciones

Esta asegura la protección de la información en las redes informáticas e instalaciones de procesamiento de la información de apoyo.

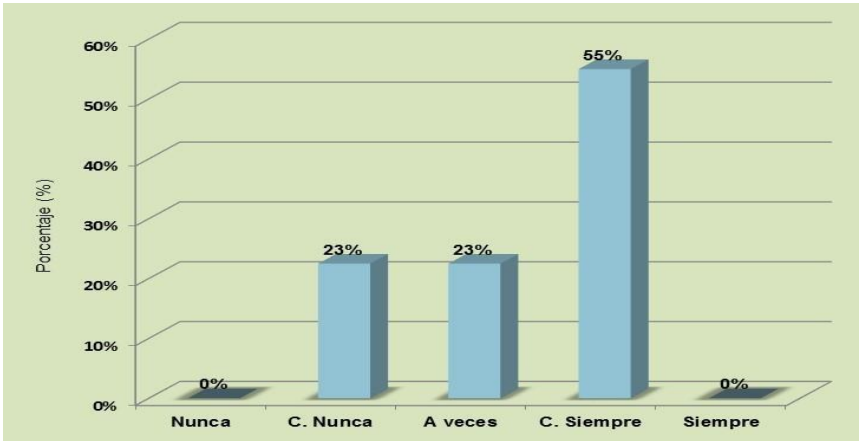

Figura 27. Revisión de información confidencial o importanteantes de ser destruida y desechable.

Un 55% de los entrevistados afirmaron que casi siempre es cuidadoso en arrojar información confidencial o de vital importancia en el depósito de basura sin su destrucción previa, mientras que el restante 23% declaró como casi un nunca y a veces, lo que evidencia que los controles aplicados ayudan a que la misma se encuentre bien protegida y no susceptible de caer en manos de la competencia o en las de posibles ciberdelincuentes.

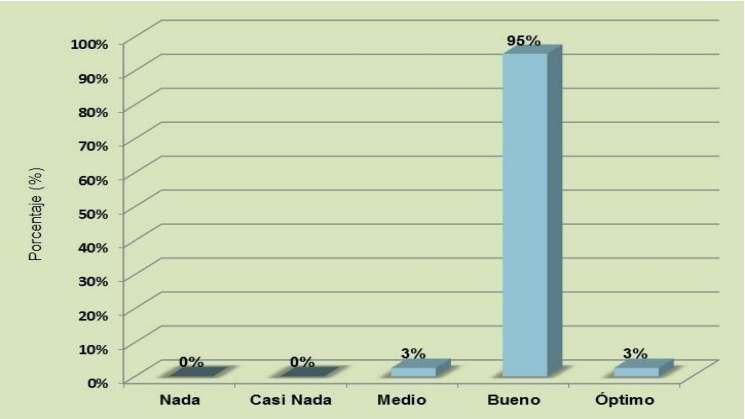

Figura 28. Mantenimiento de los registros de auditoria al procesamientode la información no autorizada.

El 95% de los entrevistados afirmaron que son buenos y el restante 3% como óptimo son los registros de auditoria utilizados por la empresa Redondos, S.A., al momento de detectar alguna actividad de procesamiento de información que no ha sido autorizada, a su vez se tienen requisitos bien definidos para los acuerdos de confidencialidad o no divulgación de la organización, así también, la protección de la información, donde se identifican, revisa regularmente y los mismos son documentados.

Dominio: Adquisición, desarrollo y mantenimiento de sistemas

Este busca a garantizar la seguridad de la información como parte integral a través del ciclode vida. Incluyendo los requisitos del sistema de información que proporcionen servicios sobre redes públicas.

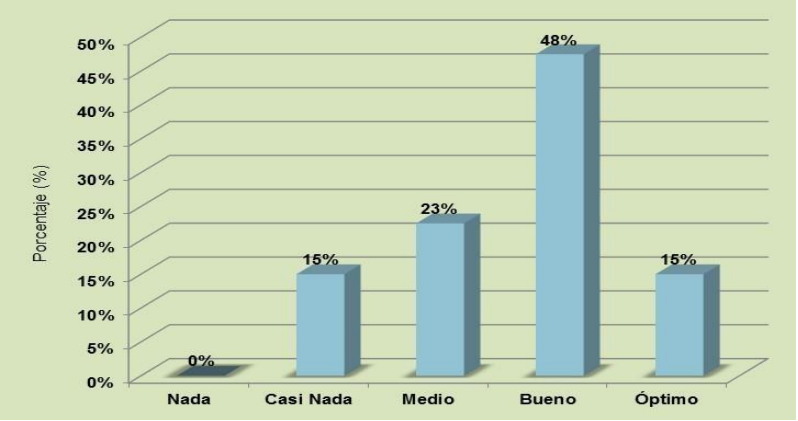

Figura 29. Análisis y especificaciones de seguridad en la mejora o nuevos sistemas de información.

un 48% de los entrevistados afirman como bueno, el 15% como óptimo y casi nada y el restante 23% en término medio, consideran que si se realizan los análisis y especificacionesde seguridad para los sistemas de información nuevos o en su defecto a los ya existentes, a su vez cuando se realiza cualquier cambio en las plataformas operativas, no son del todo revisadas las aplicaciones críticas lo que genera ocasionalmente un impacto adverso en las operaciones o en la seguridad de la organización.

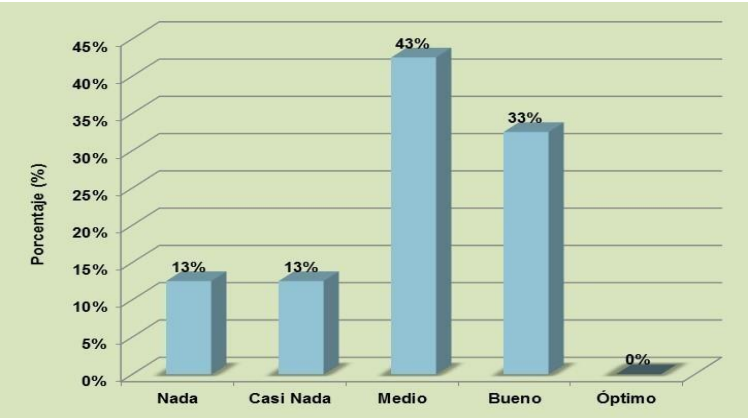

Figura 30. Aplicaciones que ayuden a comprobar y detectarcualquier corrupción de la información.

El 43 y 33% de los entrevistados afirmaron que de medio a bueno se tienen incorporadolas diferentes aplicaciones que ayudan a la comprobación y detección de síntomas de corrupción de la información, mientras que el restante 13% nada y casi nada

evidenciándose que en la empresa poco se supervisa cada uno de los mensajes de correo electrónico confidencial de los empleados, se recolectan informaciones personales sobre los individuos cada vez que ellos visitan un sitio en la world wide web, entre otras acciones.

Dominio: Relaciones con los proveedores

Este busca asegurar la protección a los activos de la empresa, accesibles a los proveedores.

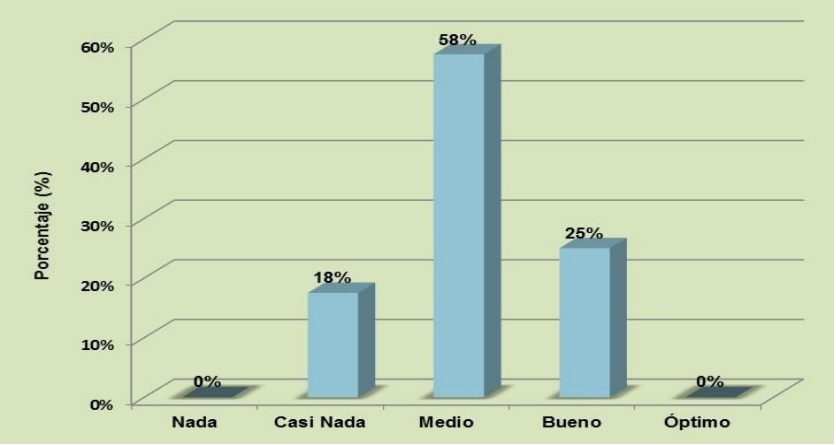

Figura 31. Política de seguridad de información para acceso a los proveedores.

El 58% afirmó que medianamente en la empresa Redondos, S.A., se tienen políticas de seguridad en cuanto a lineamientos y relación con los proveedores, el 25% que son buenos yel restante 18% en casi nada, es por ello que es necesario afinar políticas que permitan mitigar parte de los riesgos asociados con el acceso del proveedor a los activos de la empresa, a través de acuerdos subscritos documentados.

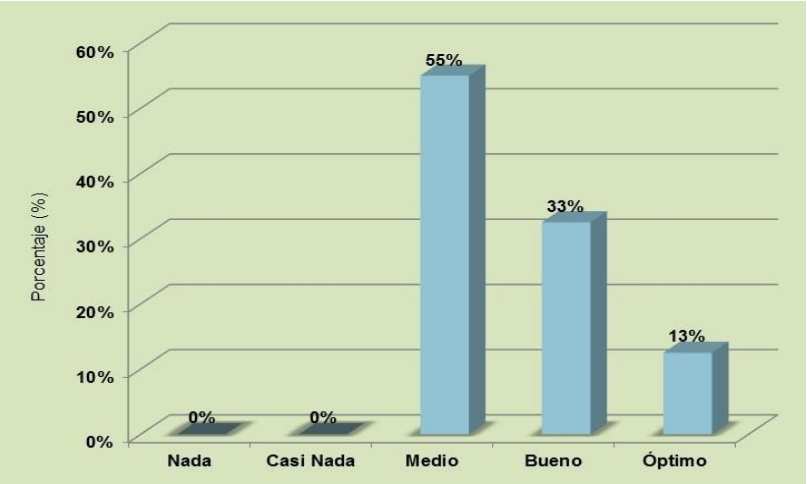

Figura 32. Implementación de planes de mantenimiento y recuperación de operaciones con los proveedores a la disponibilidad de la información.

El 55% de los entrevistados declaró como medio, el 33% como bueno y el 13% como óptimo se encuentran desarrollados e implementados planes para mantener y recuperar las operaciones con los diferentes proveedores y asegurar la disponibilidad de la información en los plazos requeridos, quedando evidenciado que la empresa debe fortalecer aún más sus procesos de monitoreo, auditorias y revisión regular para mejorar sus operaciones en relación con sus proveedores.

Dominio: Gestión de los incidentes de seguridad de la información

Este busca asegurar la consistencia y efectividad de la gestión de incidentes de seguridad de la información, así como también, la comunicación de los eventos de seguridad y debilidades.

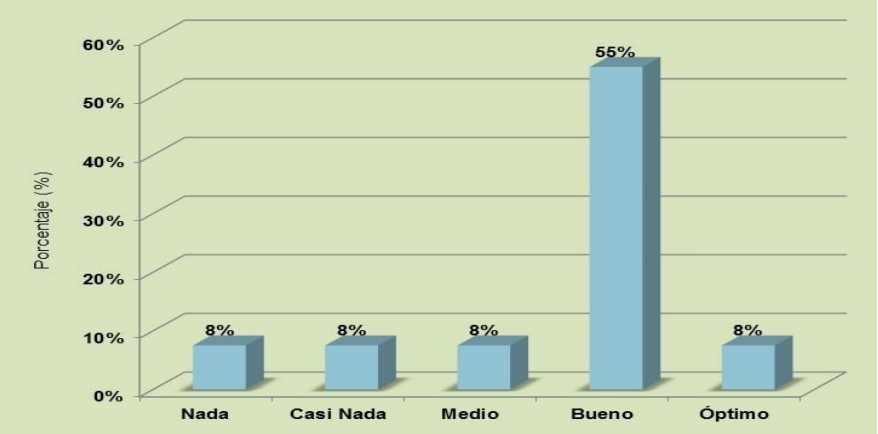

Figura 33. Reporte de debilidades de la seguridad de la información y servicios.

El 55% de los empleados afirmaron que tanto ellos como el personal contratista que hacen uso de los sistemas de información se les exige a reportar cualquier debilidad o sospecha en cuanto de la seguridad de la información en los sistemas o servicios, mientras que el restante 8% declaró que, en nada, casi nada, medio y óptimo.

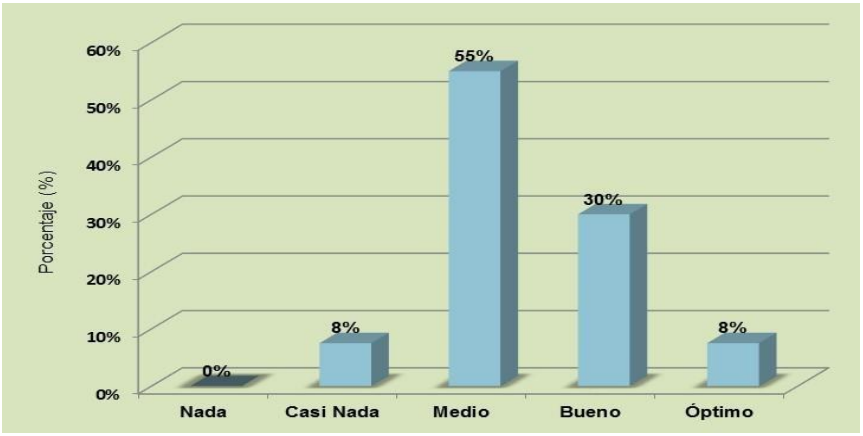

Figura 34. Responsabilidades y procedimiento de gestión a respondera los incidentes de seguridad de información.

El 55% de los entrevistados afirmaron como medio, el 30% como bueno y el restante 8% como casi nada y óptimo son las políticas establecidas en responsabilidades y procedimientos de gestión que busquen a asegurar que la respuesta al momento de ocurrir algún incidente de información se haga de forma eficaz y ordenada.

Dominio: Aspectos de seguridad de la Información de la Gestión de la continuidad del Negocio.

Asegura la continuidad de seguridad de la información en los sistemas de gestión de continuidad del negocio de la información.

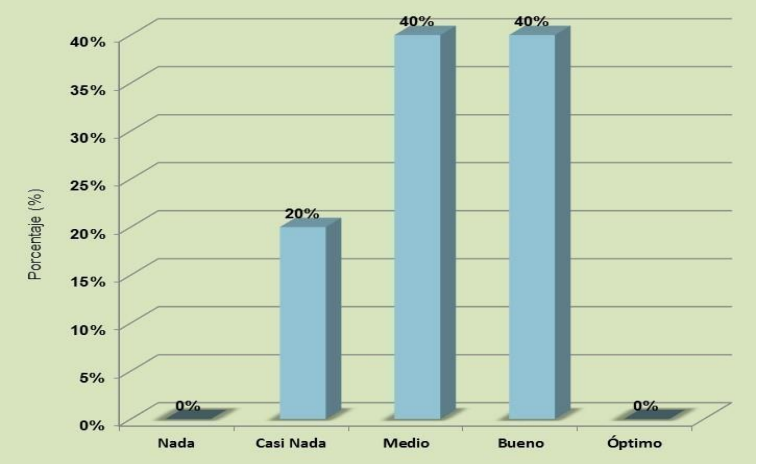

Figura 35. Mecanismos de seguridad de la información en situaciones adversasa la disponibilidad de los servicios de tecnología de información.

El 40% de los entrevistados afirmaron que de medio a óptimo se encuentran los mecanismos usados por la empresa que den evidencia la seguridad de la información en circunstancias a la no disponibilidad de los servicios de tecnología de información, mientras que el restante 20% en casi nada, estos ayudan a determinar a través de sus requisitos de seguridad de la información las sensibilidades que se puedan presentar durante una crisis o desastre y así buscar la mitigación de la misma.

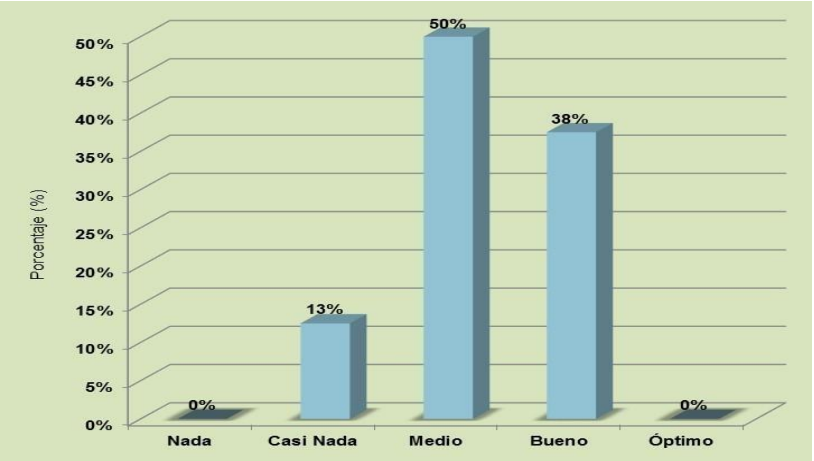

Figura 36. Identificación de interrupciones a los procesos e impactoen la seguridad de la información.

El 50% declaró como medio, el 38% como bueno y el 13% como casi nada se identifican cada uno de los eventos ocurridos de interrupciones a los procesos llevados por la empresa, es por ello que es necesario revisar y mejorar cada uno de los controles aplicado que ayudena optimizar estos procesos y aseguramiento de continuidad de la seguridad de la información durante una situación adversa a través de la identificación de los mismos y sus planes de mitigación.

Dominio: Cumplimiento.

Este busca a evitar infracciones de las obligaciones legales, estatuarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.

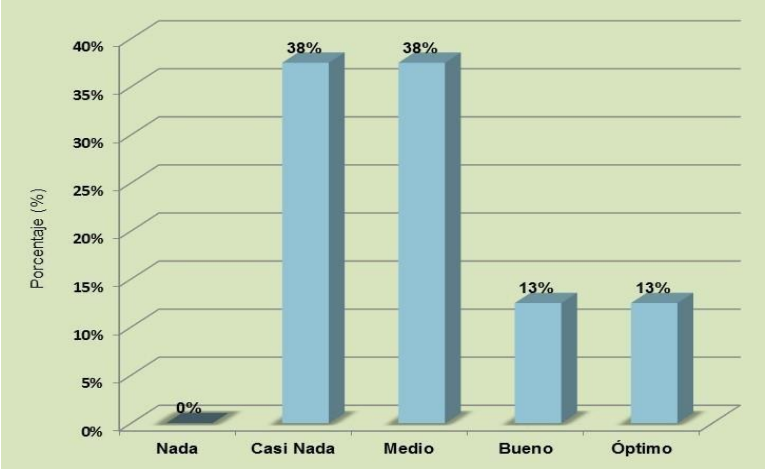

Figura 37. Requisitos legales, reglamentarios y contractualesen cada sistema de información.

.

El 38% afirmó que de medio a casi nada y el restante 13% de bueno a óptimo se encuentran definidos, documentados y actualizados todos los requisitos legislativos, estatuarios, regulatorios, y contractuales relevantes para cada sistema de información, evidenciándose el gran descuido que esta tiene para la empresa que pueden generar sanciones legales por algún incumplimiento.

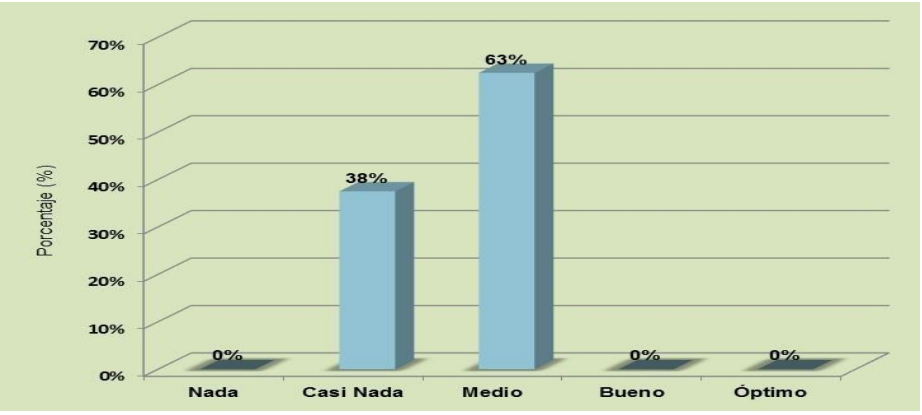

Figura 38. Procedimientos apropiados para asegurarse del cumplimiento de requisitos.

El 63 y 38 % afirmó que la empresa cuenta con pocos procedimientos para asegurar el cumplimiento de los requisitos antes mencionados.

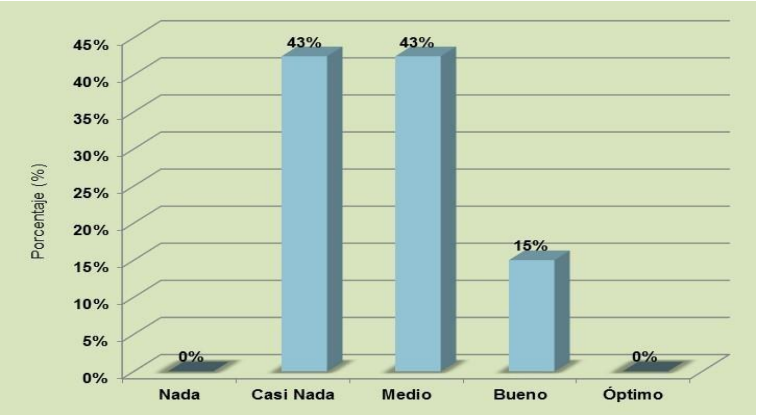

Figura 39. Protección de registros contra pérdidas, destrucción y falsificación.

El 43% afirmó la poca importancia que la empresa protegidos por perdida. De acuerdo con los requisitos legislativos, regulatorios y contractuales y del negocio.

El análisis de riesgos se ejecuta bajo el marco de la gestión integral del riesgo institucional.El alcance del análisis de riesgos es el del Sistema de Gestión de Seguridad de la Información (SGSI), es decir, un conjunto de activos de información (Ai), que asisten a los procesos institucionales (Pk).

El riesgo resultante se clasifica en los niveles mostrados en la siguiente figura:

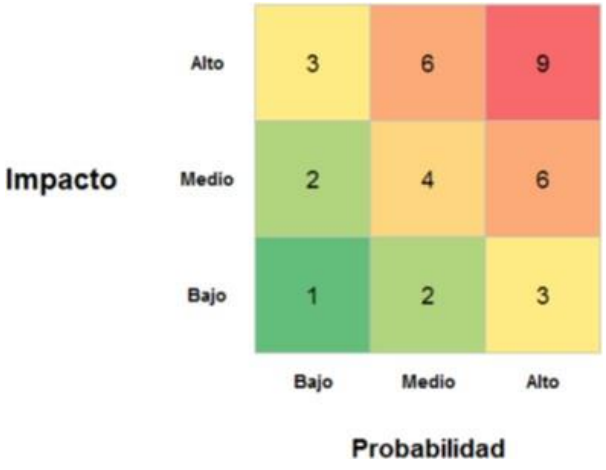

Figura 40. Mapa de riesgos.
Fuente. INCIBE.

Tabla 1

Valoración de probabilidad

TABLA PARA ESTIMAR LA PROBABILIDAD	
VALOR	**DESCRIPCIÓN**
Bajo (1)	La amenaza se materializa a lo sumo una vez cada año.
Medio (2)	La amenaza se materializa a lo sumo una vez cada mes.
Alto (3)	La amenaza se materializa a lo sumo una vez cada semana.

Fuente. INCIBE.

Tabla 2

Valoración del impacto

TABLA PARA ESTIMAR EL IMPACTO	
VALOR	**DESCRIPCIÓN**
Bajo (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio (2)	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto (3)	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Fuente. INCIBE.

Nivel de aceptación o tolerancia al riesgo

Tabla 3

Valoración del nivel de aceptación / tolerancia

CRITERIOS DE ACEPTACIÓN DEL RIESGO	
RANGO	**DESCRIPCIÓN**
Riesgo <= 4	La organización considera el riesgo poco reseñable.
Riesgo > 4	La organización considera el riesgo reseñable y debe proceder a su tratamiento.

Fuente. INCIBE.

Valoración de los procedimientos y controles para el monitoreo y revisión del sistema de información en base a los criterios de la norma ISO 27001.

Manejo de la información (Empresa Redondos S.A)

En la tabla se muestra los nombres de los ERP'S y aplicaciones de desarrollos con los que actualmente cuenta la empresa Redondos, S.A., así mismo describe el manejo que realiza cadauno de estos sistemas:

Tabla 4.

ERP'S y aplicaciones de desarrollos de la empresa Redondos, S.A.

Manejo de información	**Descripción**
ERP mtech	Nuevos usuarios, (Creación por el área tecnologías de la información). Ingreso de información: ▪ Reproductora ▪ Incubación ▪ Planta Alimento ▪ Engorde Operaciones de contabilidad. Gestión compra de producto. Gestión Venta de producto Reportes.
ERP dynamics	Nuevos usuarios, (Creación por el área tecnologías de la información). Contabilidad Activos fijos Tesorería Procesos financieros Planificación de suministros Gestión de presupuestos Crear y consolidar informes

	Adjuntar comentarios a los registros de empleados Realización de seguimiento de los costes y los consumos Reportes.
ERP ofisis	Nuevos usuarios, (Creación por el administrador del área recursos humanos). Administración de Planillas Administración de Contratos Administración de Vacaciones Cuenta Corriente (Adelantos y préstamos al personal) Periodos de pago flexibles Reportes
Sistema sispro	Nuevos usuarios, (Creación por el administrador del sistema, Planta procesamiento). Plan de ventas. Plan producción y capacidad Plan de requerimientos de materiales Plan de producción Producción Reportes
Sistema producción de alimento balanceado.	Nuevos usuarios (Creación por el administrador de sistema, Planta alimentos). Registro de insumos Registro de líneas de producción Registro de prensas Registro de tolvas Reportes
Qlikview viewer	Nuevos usuarios, (Creación por el área tecnologías de la información). Consolidando datos útiles Toma de decisiones Informes Consultas y construcción de cubos.

Intranet	Nuevos usuarios, (Creación por el área tecnologías de la información). Registro Tarea Huacho Búsqueda de Deuda Tramite Documentario Gestión Documentaria Gestión de la Calidad
Sistema de inventario	Nuevos usuarios, (Creación por el área tecnologías de la información). Registro de Activos. Reportes

Identificación de riesgo

Tabla 5

Activos de información de la empresa Redondos, S.A.

Nombre	Descripción	Categoría	Ubicación	Propietario
Aplicaciones	Office 2007, 2010, 2013, 2016. Opens Office. Adobe Reader Project Visio Autocad Virtual Network Computing Network Connect Antivirus Sophos	Aplicaciones	Servidor	Tecnología de la Información
Sistemas operativos equipos de escritorio	Windows 7, 8, 8.1, 10, Professional.	Software	Servidor	Tecnología de la Información
Sistemas operativos servidores	Windows Server: 2003, 2008, 2012, 2016.	Software	Servidor	Tecnología de la Información

Dispositivos de Almacenamiento.	Discos externos.	Dispositivos	Área T.I	Tecnología de la Información
Aplicaciones desarrolladas	Intranet Ssispro Gestión de incidencias Scada Sistema de tienda Sistema avícola	Aplicaciones	Servidor	Tecnología de la Información
Equipos de Usuario	Desktops Laptops Impresoras, scanners.	Hardware	Redondos S.A	Tecnología de la Información
Servidores	ERP´s Base datos Backup Aplicaciones.	Hardware	Redondos S.A	Tecnología de la Información
Correo Electrónico	Correo Electrónico	Subcontratación	Microsoft	Redondos S.A
Servicios	Internet, Radioenlaces, teléfonos corporativos, Energía Eléctrica.	Subcontratación	Redondos S.A	Redondos S.A
Usuarios	Datos de usuarios	Datos	Servidor	Tecnología de la Información

Valoración de activos

Para realizar la valoración de activos fue necesario aplicar el instrumento diseñado para recolectar la información necesaria basado en cada una de las dimensiones establecidas por la metodología Magerit (ver anexo A), se hizo el levantamiento en base a las respuestas por el áreade tecnologías de la información, se promedió y se procedió a organizarlos de forma resumida en la siguiente tabla.

Tabla 6. Escala de valorización de los activos de la empresa Redondos, S.A.

Activos	Confidencial	Integridad	Disponibilidad	Total
Aplicaciones	2	3	4	9
Sistemas operativos equipos de escritorio	2	3	4	9
Sistemas operativos servidores	3	3	4	10
Dispositivos de Almacenamiento.	4	4	4	12
Aplicaciones desarrolladas	3	3	4	10
Equipos de Usuario	2	3	4	9
Servidores	4	4	4	12
Correo Electrónico	3	3	4	10
Servicios	3	4	4	11
Usuarios	2	3	4	9

Nivel	Criterio
10	Nivel 10
9	Nivel 9
8	Nivel 8 +
7	Alto
6	Alto -
5	Medio
4	Medio +
3	Medio -
2	Bajo +
1	Bajo
0	Despreciable

Figura 40. Criterios de evaluación

Identificación de amenazas, seguridad de la información

Los activos están expuestos a amenazas, presentadose con una frecuencia o probabilidad, la cual en muchos de los casos dependerá de la eficacia de la aplicación de los controles. Ahora bien, a fin de determinar los riesgos, se empleó el catálogo de amenazas de MAGERIT, Instituto Nacional de Ciberseguridad (INCIBE). Así como también las vulnerabilidades y controles identificados por los administradores de activos, con base en su experiencia e información de los fabricantes. Las amenazas se organizan en categorías consignadas en la figura 35, y pueden afectar a más de un tipo de activo.

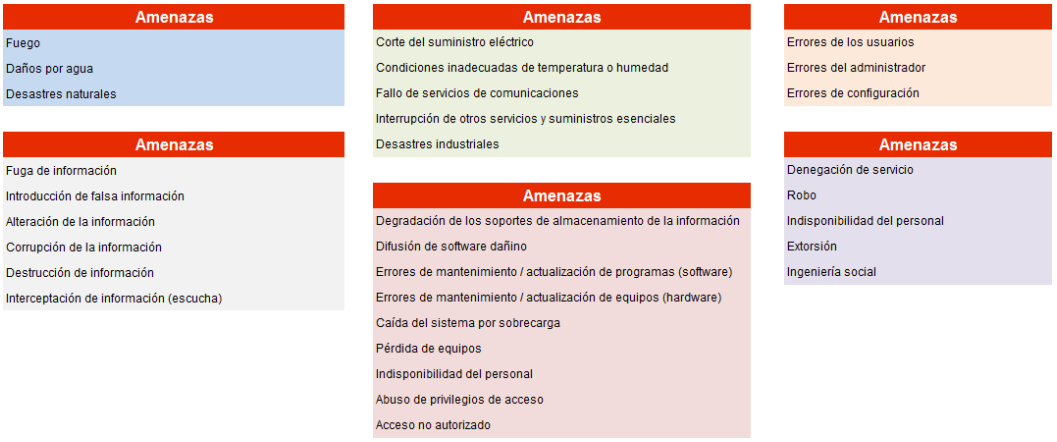

Figura 41: Catálogos de amenazas

Fuente. INCIBE.

Estimación de Riesgos

Para realizar la estimación de riesgo se procedió en primera instancia a construir el instrumento cualitativo (ver anexo B), el mismo se aplicó a la muestra seleccionada constituidapor cuarenta empleados de la empresa Redondos, S.A., en la misma se pudo visualizar la apreciación de estos en base a los criterios que la misma metodología exige que sean estudiados,como lo son el impacto y probabilidad, con la finalidad de poder determinar el riesgo total en base a cada una de las amenazas a los cuales está sometido los activos de información, una vezobtenidos los datos se organizaron en la tabla mostrada a continuación.

Tabla 7
Resultados de los riesgos
Tratamiento de riesgo

ANÁLISIS DE RIESGOS				
Activo	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
ordenador(es)	Fuego	Bajo (1)	Alto (3)	3
ordenador(es)	Daños por agua	Bajo (1)	Bajo (1)	1
ordenador(es)	Desastres naturales	Bajo (1)	Alto (3)	3
ordenador(es)	Fuga de información	Bajo (1)	Alto (3)	3
ordenador(es)	Introducción de falsa información	Bajo (1)	Alto (3)	3
ordenador(es)	Alteración de la información	Bajo (1)	Alto (3)	3
ordenador(es)	Corrupción de la información	Bajo (1)	Alto (3)	3
ordenador(es)	Destrucción de información	Bajo (1)	Alto (3)	3
ordenador(es)	Interceptación de información (escucha)	Bajo (1)	Alto (3)	3
ordenador(es)	Corte del suministro eléctrico	Bajo (1)	Medio (2)	2
ordenador(es)	Condiciones inadecuadas de temperatura o humedad	Bajo (1)	Bajo (1)	1
ordenador(es)	Fallo de servicios de comunicaciones	Bajo (1)	Medio (2)	2
ordenador(es)	Interrupción de otros servicios y suministros esenciales	Bajo (1)	Medio (2)	2
ordenador(es)	Desastres industriales	Bajo (1)	Alto (3)	3
ordenador(es)	Degradación de los soportes de almacenamiento de la información	Bajo (1)	Alto (3)	3
ordenador(es)	Difusión de software dañino	Bajo (1)	Bajo (1)	1
ordenador(es)	Errores de mantenimiento / actualización de programas	Bajo (1)	Alto (3)	3
ordenador(es)	Errores de mantenimiento / actualización de equipos (hardware)	Bajo (1)	Alto (3)	3
ordenador(es)	Caída del sistema por sobrecarga	Bajo (1)	Alto (3)	3
ordenador(es)	Pérdida de equipos	Bajo (1)	Medio (2)	2
ordenador(es)	Indisponibilidad del personal	Medio (2)	Bajo (1)	2
ordenador(es)	Abuso de privilegios de acceso	Medio (2)	Bajo (1)	2
ordenador(es)	Acceso no autorizado	Bajo (1)	Medio (2)	2
ordenador(es)	Errores de los usuarios	Medio (2)	Bajo (1)	2
ordenador(es)	Errores del administrador	Medio (2)	Bajo (1)	2
ordenador(es)	Errores de configuración	Bajo (1)	Medio (2)	2
ordenador(es)	Denegación de servicio	Bajo (1)	Medio (2)	2
ordenador(es)	Robo	Bajo (1)	Alto (3)	3
ordenador(es)	Indisponibilidad del personal	Bajo (1)	Bajo (1)	1
ordenador(es)	Extorsión	Bajo (1)	Medio (2)	2
ordenador(es)	Ingeniería social	Bajo (1)	Bajo (1)	1

Debido a que el valor de riesgo resultó aceptable se les dará tratamiento los que igualan o superan esta cifra y se asumen los que están por debajo de este, de igual forma se deben aplicarcontroles mínimos de acuerdo a lo establecido en la norma, los resultados se muestran en la tabla 8.

Tabla 8

Tratamiento de riesgos

Amenaza	Riesgo	Tratamiento
Fuego	3	Se asume
Daños por agua	1	Se asume
Desastres naturales	3	Se asume
Fuga de información	3	Se asume
Introducción de falsa información	3	Se asume
Alteración de la información	3	Se asume
Corrupción de la información	3	Se asume
Destrucción de información	3	Se asume
Interceptación de información (escucha)	3	Se asume
Corte del suministro eléctrico	2	Se asume
Condiciones inadecuadas de temperatura o humedad	1	Se asume
Fallo de servicios de comunicaciones	2	Se asume
Interrupción de otros servicios y suministros esenciales	2	Se asume
Desastres industriales	3	Se asume
Degradación de los soportes de almacenamiento de la información	3	Se asume
Difusión de software dañino	1	Se asume
Errores de mantenimiento / actualización de programas (software)	3	Se asume
Errores de mantenimiento / actualización de equipos (hardware)	3	Se asume
Caída del sistema por sobrecarga	3	Se asume
Pérdida de equipos	2	Se asume
Indisponibilidad del personal	2	Se asume
Abuso de privilegios de acceso	2	Se asume
Acceso no autorizado	2	Se asume

Errores de los usuarios	2	Se asume
Errores del administrador	2	Se asume
Errores de configuración	2	Se asume
Denegación de servicio	2	Se asume
Robo	3	Se asume
Indisponibilidad del personal	1	Se asume
Extorsión	2	Se asume
Ingeniería social	1	Se asume

Declaración de aplicabilidad

Controles aplicados

Por medio de los controles aplicados se establecen los lineamientos establecidos por la norma ISO 27001:2013 en su anexo A, que ayudarán a salvaguardar los activos de la empresa Redondos, S.A.

4. Análisis y discusión

En el estudio se utilizó la Norma ISO 27001: 2013, con la finalidad de proteger la información de la empresa, aplicando controles y procedimientos bajo un criterio empresarial, se aplicó instrumentos de recolección de datos en la identificación de riesgo, para luego valorar y minimizar las deficiencias que se presentan. Así mismo, Para un mejor control del sistema de información se establecieron los controles y procedimientos, considerando los criterios establecidos según la norma

Se encontró similitud con el estudio de Alcántara (2015), respecto a la seguridad en los diferentes efectos se apoyó de acuerdo a los criterios establecidos en la norma NTP ISO/IEC 27001, asimismo, en el diseño de implementación del sistema de gestión de seguridad de información coincide con los fundamentos aportados por Barrantes y Hugo (2012),logro reducir y mitigar los riesgos de los activos de la empresa utilizando Magerit para poder proteger los activos de información,

Además, guarda afinidad con la investigación de Guzmán (2015) respecto a las normas en el diseño de un sistema Gestión de seguridad de la información, se coincide con el tipo de investigación, concerniente a los mecanismos e instrumentos para la recolección de información; cuestionario, observaciones y entrevistas al personal del área de tecnología de la entidad, por otro lado, es de recalcar que, se encontró similitud a lo aplicado en los procedimientos del proyecto elaborado por Nieves (2017) para finalmente hacer un diseño de seguridad de información, asegurando la integridad y continuidad de los servicios (al igual en los equipos y sistemas de información, para así poder darle un uso adecuado en temas de seguridad de la entidad. Tambiéncoincidiendo en el uso de la misma norma, ISO/IEC 27001, utilizada por Olaza (2017), en la cual se aseguró la confidencialidad, así mismo la integridad y disponibilidad de los sistemas deinformación fueron empleados en este estudio

5. Conclusiones y Recomendaciones

Para el desarrollo de la presente investigación fue fundamental realizar una serie de actividadeslo cual permitió cumplir con cada uno de los objetivos que se trazaron para llevar a cabo la presente investigación. Ya terminado el desarrollo de la investigación se tienen las siguientes conclusiones:

- Se identificaron los riesgos que se encuentran sometidos los sistemas de información manejados por la empresa Redonda, S.A., mediante la aplicación de instrumentos de recolección y analizado la información se obtuvo riegos ≤ 4, catalogados para la organización como riesgos poco reseñables.
- Se valoró los riesgos, resultando aceptable para tratamiento para aplicar controles mínimos de acuerdo a lo establecido en la norma ISO 27001: 2013
- Se establecieron los procedimientos y controles mediante la declaración de aplicabilidad en base al criterio del anexo A de la normala cual permitió presentar las consideraciones de la mejora de los procesos del área quefueron vulnerados y que se considera cuentan con cierto nivel de riesgo en sus procesos operativos.

Recomendaciones

- Aplicar técnicas de recolección de información para detectar los riesgos que se presentan en la Seguridad de la información a nivel empresarial y salvaguardar la información que posee la organización, a fin de mantener la información de acuerdo al lineamiento establecidos en la norma ISO 27001: 2013.
- Analizar periódicamente los controles aplicados en base a los requerimientos de la organización y de acuerdo a lo que se dispone en seguridad de la información para el levantamiento de la información del sistema de gestión de seguridad de la información,ya que esta permitirá identificar los activos de información, así como el diagnostico de seguridad de los mismos.
- Una vez revisados estos controles aplicar nuevamente el análisis de riesgos con la finalidad de que todos puedan llegar al nivel bajo.

6. Referencias Bibliográficas

Aguilera E.(2015). *Normas ISO 27001*. Disponimbe en: https://es.slideshare.net/edicksonaguilera/norma-iso-27001autor-edickson-aguilera

Alcantara J. (2015). *Guía de implementación de la seguridad basado en la norma iso/iec27001, para apoyar la seguridad en los sistemas informáticos de la comisariadel norte P.N.P en la ciudad de Chiclayo*. Universidad Católica Santo ToribioDe Mogrovejo, Perú. Retrieved From http://tesis.usat.edu.pe/bitstream/usat/539/1/TL_Alcantara_Flores_JulioCesar.p df

Barrantes C y Hugo J. (2012). *Diseño e implementación de un sistema de gestión deseguridad de información en procesos tecnológicos*. Universidad San Martin dePorres, Perú. Retrieved From http://repositorio.ucv.edu.pe/bitstream/handle/UCV/9927/Olaza_AHD.pdf?seq uence=1

Isotool. (s.f). Isotools Excel. Recuperado de: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

Kosutic D. (2015). *Que es Norma ISO 27001*. Disponible en:https://advisera.com/27001academy/es/que-es-iso-27001/ https://advisera.com/27001academy/knowledgebase/how-to-make-a-transition- from-iso-27001-2005-revision-to-2013-revision/

Gutierres C. (24 mayo 2013). *Metodología practica para gestionar riesgos. Disponible en* : https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia- practica-para-gestionar-riesgos/

Guzmán C. (2015). *Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso*. Institución Universitaria Politécnico Grancolombiano, Colombia. Retrieved From https://www.dspace.espol.edu.ec/retrieve/89073/D-84631.pdf.

Nieves A. (2017). *Diseño de un sistema de gestión de la seguridad de la información (sgsi) basados en la norma ISO/IEC 27001:2013*. Politécnico

Grancolombiano,Colombia. Retrieved From http://repository.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?sequence=1&isAllowed=y

Olaza H. (2017). *Implementación de NTP ISO/IEC 27001 para la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación - Sede Centromin. Universidad Cesar Vallejo, Peru*. Retrieved From http://repositorio.ucv.edu.pe/bitstream/handle/UCV/9927/Olaza_AHD.pdf?sequence=1&isAllowed=y

Olivera M. (2016). *Principales Novedades de la ISO 27001/ISO 27002*.disponible en:https://docplayer.es/971903-Principales-novedades-de-la-iso-27001-iso-27002.html

7. Anexos.

Anexo: Código de buenas prácticas para la gestión de la seguridad de la información.

ISO 27001 Anexo A. Dominios, objetivos de control.

5. Política de Seguridad.
   - 5.1. Política de seguridad de la información.
     - 5.1.1. Documento de política de seguridad de la información.
     - 5.1.2. Revisión de la política de seguridad de la información.
6. Aspectos Organizativos.
   - 6.1. Organización interna.
     - 6.1.1. Comité de gestión de seguridad de la información.
     - 6.1.2. Coordinación de la seguridad de la información.
     - 6.1.3. Asignación de responsabilidades de la seguridad de la información.
     - 6.1.4. Proceso de autorización de recursos para proceso de información.
     - 6.1.5. Acuerdos de confidencialidad.
     - 6.1.6. Contacto con las autoridades.
     - 6.1.7. Contacto con grupos de especial interés.
     - 6.1.8. Revisión independiente de la seguridad de la información.
   - 6.2. Terceros.
     - 6.2.1. Identificación de los riesgos derivados del acceso de terceros.
     - 6.2.2. Tratamiento de seguridad en la relación con los clientes.
     - 6.2.3. Tratamiento de seguridad en contratos con terceros (*outsourcing*).
7. Gestión de activos.
   - 7.1. Responsabilidad sobre los activos.
     - 7.1.1. Inventario de activos.
     - 7.1.2. Propiedad de los activos.
     - 7.1.3. Uso aceptable de los activos.
   - 7.2. Clasificación de la información.
     - 7.2.1. Directrices de clasificación.
     - 7.2.2. Etiquetado y manipulado de la información.
8. Seguridad ligada a los recursos humanos.
   - 8.1. Antes del empleo.
     - 8.1.1. Funciones y responsabilidades.
     - 8.1.2. Investigación de antecedentes.
     - 8.1.3. Términos y condiciones de contratación.
   - 8.2. Durante el empleo.
     - 8.2.1. Responsabilidades de la Dirección.
     - 8.2.2. Concienciación, formación y capacitación en seguridad de la inform.
     - 8.2.3. Proceso disciplinario.
   - 8.3. Cese del empleo o cambio de puesto de trabajo.
     - 8.3.1. Responsabilidad en el cese o cambio.
     - 8.3.2. Devolución de activos.
     - 8.3.3. Retirada de los derechos de acceso.
9. Seguridad física y ambiental.
   - 9.1. Áreas seguras.
     - 9.1.1. Perímetro de seguridad física.
     - 9.1.2. Controles físicos de entrada.
     - 9.1.3. Seguridad de oficinas, despachos e instalaciones.
     - 9.1.4. Protección contra las amenazas externas y de origen ambiental.
     - 9.1.5. Trabajo en áreas seguras.
     - 9.1.6. Áreas de acceso público y de carga y descarga.
   - 9.2. Seguridad de los equipos.
     - 9.2.1. Emplazamiento y protección de equipos.
     - 9.2.2. Instalaciones de suministro.
     - 9.2.3. Seguridad del cableado.
     - 9.2.4. Mantenimiento de los equipos.
     - 9.2.5. Seguridad de los equipos fuera de las instalaciones.
     - 9.2.6. Reutilización o retirada segura de equipos.
     - 9.2.7. Retirada de materiales propiedad de la empresa.
10. Gestión de comunicaciones y operaciones.
    - 10.1. Responsabilidades y procedimientos de operación.
      - 10.1.1. Documentación de los procedimientos de operación.
      - 10.1.2. Gestión de cambios.
      - 10.1.3. Segregación de tareas.
      - 10.1.4. Separación de entornos de desarrollo, prueba y operación.
    - 10.2. Gestión de la provisión de servicios por terceros.
      - 10.2.1. Provisión de servicios.
      - 10.2.2. Supervisión y revisión de los servicios prestados por terceros.
      - 10.2.3. Gestión de cambios en los servicios prestados por terceros.
    - 10.3. Planificación y aceptación del sistema.
      - 10.3.1. Gestión de capacidades.
      - 10.3.2. Aceptación del sistema.
    - 10.4. Protección contra código malicioso y descargable.
      - 10.4.1. Controles contra el código malicioso.
      - 10.4.2. Controles contra el código descargado en el cliente.
    - 10.5. Copias de seguridad.
      - 10.5.1. Copias de seguridad de la información.
    - 10.6. Gestión de la seguridad de las redes.
      - 10.6.1. Controles de red.
      - 10.6.2. Seguridad de los servicios de red.
    - 10.7. Manipulación de los soportes.
      - 10.7.1. Gestión de soportes extraíbles.
      - 10.7.2. Retirada de soportes.
      - 10.7.3. Procedimientos de manipulación de la información.
      - 10.7.4. Seguridad de la documentación del sistema.
    - 10.8. Intercambio de información.
      - 10.8.1. Políticas y procedimientos de intercambio de información.
      - 10.8.2. Acuerdos de intercambio.
      - 10.8.3. Soportes físicos en tránsito.
      - 10.8.4. Mensajería electrónica.
      - 10.8.5. Sistemas de información empresariales.
    - 10.9. Servicios de comercio electrónico.
      - 10.9.1. Comercio electrónico.
      - 10.9.2. Transacciones en línea.
      - 10.9.3. Información puesta a disposición pública.
    - 10.10. Supervisión.
      - 10.10.1.Registro de auditorías.
      - 10.10.2.Supervisión del uso del sistema.
      - 10.10.3.Protección de la información de los registros..
      - 10.10.4.Registros de administración y operación.
      - 10.10.5.Registro de fallos.
      - 10.10.6.Sincronización del reloj.
11. Control de acceso.
    - 11.1. Requisitos de negocio para el control de acceso.
      - 11.1.1. Política de control de acceso.
    - 11.2. Gestión de acceso de usuario.
      - 11.2.1. Registro de usuario.
      - 11.2.2. Gestión de privilegios.
      - 11.2.3. Gestión de contraseñas de usuario.
      - 11.2.4. Revisión de los derechos de acceso de usuario.
    - 11.3. Responsabilidades de usuario.
      - 11.3.1. Uso de contraseña.
      - 11.3.2. Equipo de usuario desatendido.
      - 11.3.3. Política de puesto de trabajo y pantalla limpia.
    - 11.4. Control de acceso a la red.
      - 11.4.1. Política de uso de los servicios en red.
      - 11.4.2. Autenticación de usuario para conexiones externas.
      - 11.4.3. Identificación de los equipos en las redes.
      - 11.4.4. Diagnóstico remoto y protección de los puertos de configuración.
      - 11.4.5. Segregación de las redes.
      - 11.4.6. Control de conexión a la red.
      - 11.4.7. Control de encaminamiento (*routing*) de red.
    - 11.5. Control de acceso al sistema operativo.
      - 11.5.1. Procedimientos seguros de inicio de sesión.
      - 11.5.2. Identificación y autenticación de usuario.
      - 11.5.3. Sistema de gestión de contraseñas.
      - 11.5.4. Uso de los recursos del sistema.
      - 11.5.5. Desconexión automática de sesión.
      - 11.5.6. Limitación del tiempo de conexión.
    - 11.6. Control de acceso a las aplicaciones y a la información.
      - 11.6.1. Restricción del acceso a la información.
      - 11.6.2. Aislamiento de sistemas sensibles.
    - 11.7. Ordenadores portátiles y teletrabajo.
      - 11.7.1. Ordenadores portátiles y comunicaciones móviles.
      - 11.7.2. Teletrabajo.
12. Adquisición, desarrollo y mantenimiento de los sistemas de información.
    - 12.1. Requisitos de seguridad de los sistemas de información.
      - 12.1.1. Análisis y especificación de los requisitos de seguridad.
    - 12.2. Tratamiento correcto de las aplicaciones.

12.2.1. Validación de datos de entrada.
12.2.2. Control del procesamiento interno.
12.2.3. Integridad de los mensajes.
12.2.4. Validación de los datos de salida.

12.3. Controles criptográficos.

12.3.1. Política de uso de los controles criptográficos.
12.3.2. Gestión de claves.

12.4. Seguridad de los archivos de sistema.

12.4.1. Control del software en explotación.
12.4.2. Protección de los datos de prueba del sistema.
12.4.3. Control de acceso al código fuente de los programas.

12.5. Seguridad en los procesos de desarrollo y soporte.

12.5.1. Procedimientos de control de cambios.
12.5.2. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
12.5.3. Restricciones a los cambios en los paquetes de software.
12.5.4. Fugas de información.
12.5.5. Externalización (*outsourcing*) del desarrollo del software.

12.6. Gestión de la vulnerabilidad técnica.

12.6.1. Control de las vulnerabilidades técnicas.

13. Gestión de incidentes de seguridad de la información.

13.1. Notificación de eventos y puntos débiles de la seguridad de la información.

13.1.1. Notificación de los eventos de seguridad de la información..
13.1.2. Notificación de los puntos débiles de la seguridad.

13.2. Gestión de incidentes de la seguridad de la información y mejoras.

13.2.1. Responsabilidades y procedimientos.
13.2.2. Aprendizaje de los incidentes de seguridad de la información.
13.2.3. Recopilación de evidencias.

14. Gestión de continuidad del negocio.

14.1. Aspectos de seguridad en la gestión de la continuidad del negocio.

14.1.1. Inclusión de la seguridad de la información en el proceso de gestión del la continuidad del negocio.
14.1.2. Continuidad del negocio y evaluación de riesgos.
14.1.3. Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
14.1.4. Marco de referencia para la planificación de la continuidad del negocio.
14.1.5. Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio.

15. Cumplimiento.

15.1. Cumplimiento de los requisitos legales.

15.1.1. Identificación de la legislación aplicable.
15.1.2. Derechos de propiedad intelectual (DPI/*IPR*).
15.1.3. Protección de los documentos de la Organización.
15.1.4. Protección de datos y privacidad de la información personal.
15.1.5. Prevención del uso indebido de los recursos de tratamiento de la información.
15.1.6. Regulación de los controles criptográficos.

15.2. Cumplimiento de las políticas y normas de seguridad y reglamentos técnicos

15.2.1. Cumplimiento de las políticas y normas de seguridad.
15.2.2. Comprobación del cumplimiento de reglamentos técnicos.

15.3. Consideraciones sobre la auditoría de los sistemas de información.

15.3.1. Controles de auditoría de los sistemas de información.
15.3.2. Protección de las herramientas de auditoría de los sistemas de información.

Anexo: Análisis de Riesgo.

TABLA DE VALORACIÓN DE ACTIVOS

Criterio de valoración

Nivel	Criterio
10	Nivel 10
9	Nivel 9
8	Nivel 8 +
7	Alto
6	Alto -
5	Medio
4	Medio +
3	Medio -
2	Bajo +
1	Bajo
0	Despreciable

Dimensiones

Ítem	Criterio
D	Disponibilidad
I	Integridad de los datos
C	Confidencialidad de los datos

Activos	D	I	C
Aplicaciones (Ejemplo: Office 2007, 2010, 2013, 2016, Opens Office)			
Sistemas operativos equipos de escritorio (Ejemplo: Windows 7, 8, 8.1, 10, Professional)			
Sistemas operativos servidores (Ejemplo: Windows Server: 2003, 2008, 2012, 2016)			
Dispositivos de Almacenamiento (Discos externos)			
Aplicaciones desarrolladas (Ejemplo: Intranet, Ssispro, Gestión de incidencias, Scada)			
Equipos de Usuario (Ejemplo: Desktops, Laptops, etc.)			
Servidores (Ejemplo: ERP´s, Base datos)			
Correo Electrónico			
Servicios (Ejemplo: Internet, Radioenlaces, teléfonos)			
Usuarios (Datos de usuarios)			

Anexo: Encuesta

UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Autor: Nilton César Montoya Mansilla

Encuesta

El presente instrumento forma parte del trabajo de investigación titulado:

"**Diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 dirigido para la empresa Redondos S.A., Huacho"**

Por lo que solicitamos su participación, desarrollando cada pregunta de manera objetiva y veraz. La información es de carácter confidencial y reservado, ya que los resultados serán manejados solo para fines de la investigación. Agradezco anticipadamente su valiosa colaboración.

Variable: Seguridad de la información					
Política de seguridad de la Información					
Ítem	a. Nunca	b. Casi nunca	c. A veces	d. Casi siempre	e. Siempre
1. ¿Existen documentos de políticas de seguridad de información que establezcan procedimientos a seguir para cada uno de los riesgos a los que está sometida la información?					
2. ¿Cuentan con mecanismos que los ayuden a tomar acciones rápidas y de forma correctiva cuando la información se encuentra en peligro?					
Organización de seguridad de la información					
3. ¿La junta directiva y los jefes de los distintos departamentos de la empresa Redondos, S.A., entienden, apoyan y llevan de					

forma eficaz las políticas de seguridad de la información dentro de la organización?					
4. ¿La junta directiva y los demás implicados se preocupan de que el resto del personal tenga conciencia sobre la importancia de la seguridad de la información y las responsabilidades que cada uno tiene dentro de este tema?					
5. ¿Se tienen definidos e implementados los procesos que generen la autorización de recursos de procesamiento de la información?					
Seguridad en los recursos humanos					
6. ¿Cuentan con mecanismos de verificación de los antecedentes de cada uno de los candidatos que ocupan o buscan a ocupar diferentes cargos dentro de la organización?					
7. ¿Se aplican procesos disciplinarios a los usuarios que cometan un incumplimiento de seguridad de información?					
8. ¿Se realiza el retiro de los derechos de acceso de los empleados, contratistas o usuarios de la información y los recursos una vez terminado su empleo, contrato o acuerdo dentro de la empresa?					
Gestión de activos					
9. ¿Existen mecanismos de identificación de cada uno de los activos utilizados en la empresa Redondos, S.A., que contengan informaciones tales como: nombre del departamento u oficina, teléfono, serial del equipo, ¿entre otros?					
10. ¿Se realizan inventarios en cada oficina de los equipos informáticos y de comunicación, con el serial del equipo, software instalado, usuario asignado, ubicación, entre, otros?					
11. ¿Se generan directrices para clasificar la información de acuerdo con su valor, requisitos legales, sensibilidad y criticidad para la empresa Redondos, S.A.?					
Control de accesos					
12. ¿Existen procedimientos formales de registros de usuarios para conceder y revocar el acceso a los sistemas y servicios de información?					
13. ¿Se controla la asignación de contraseñas de usuarios que busquen prevenir el acceso no autorizado a los sistemas de información?					
14. ¿Existen mecanismos que motiven al personal a tener buenas prácticas de seguridad para la selección y uso de sus contraseñas?					

Criptografía					
15. ¿Existen medios criptográficos que buscan proteger la confidencialidad, autenticidad o integridad de la información en la empresa?					
Seguridad física y del entorno					
16. ¿En la empresa se establecen de forma adecuada diferentes parámetros de seguridad a las áreas que contienen la información y las instalaciones de procesamiento de la información?					
17. ¿Se encuentran diseñados y se aplican controles de entrada apropiados a las áreas de seguridad con la finalidad de asegurar que el permiso de acceso se haga sólo a personal autorizado?					
18. ¿Existen controles de ingreso a las oficinas después del horario normal de trabajo?					
Seguridad en las operaciones					
19. ¿Existen procedimientos operativos bien documentados, mantenidos y se encuentran disponibles a todos los usuarios que los necesiten?					
20. ¿Se controlan cambios de los recursos y sistemas de procesamiento de la información?					
Seguridad en las comunicaciones					
21. ¿Se tiene el sumo cuidado de no arrojar información confidencial o de vital importancia en las papeleras sin ser destruida previamente?					
22. ¿Se producen y mantienen los registros de auditoria cuando se detectan actividades de procesamiento de la información no autorizada, a fin de ayudar a futuras investigaciones y seguimiento de control de acceso?					
Adquisición, desarrollo y mantenimiento de sistemas					
23. ¿Se realizan análisis y especificaciones de seguridad para los nuevos sistemas de información o para las mejoras de los sistemas existentes?					
24. ¿Tienen incorporados aplicaciones que ayuden a comprobar y detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados?					
Relaciones con los proveedores					
25. ¿Existe una política de seguridad en cuanto a los lineamientos de seguridad para la relación con los proveedores con el propósito de evitar accesos no autorizados a la información?					

26. ¿Se desarrollan e implementan planes para mantener y recuperar las operaciones con los diferentes proveedores y asegurar la disponibilidad de la información al nivel requerido y en los plazos requeridos?					
Gestión de los incidentes de seguridad de la información					
27. ¿Se les solicita a todos los usuarios de los sistemas y servicios de información reportar cualquier debilidad en la seguridad de los sistemas y servicios, que hayan sido observado o sospechados?					
28. ¿Se establecen responsabilidades y procedimiento de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de información?					
Aspectos de seguridad de la Información de la Gestión de la continuidad del Negocio					
29. ¿Existen mecanismos que den evidencia la seguridad de la información en situaciones adversas que puedan comprometer la disponibilidad de los servicios de tecnología de información?					
30. ¿Se identifican los eventos que pueden causar las interrupciones a los procesos de la empresa Redondos, S.A., al mismo tiempo que la probabilidad e impacto de tales interrupciones y sus consecuencias para la seguridad de la información?					
Cumplimiento					
31. ¿Se definen, documentan y se actualizan todos los requisitos legales, reglamentarios y contractuales, para cada sistema de información de la empresa Redondos, S.A.?					
32. ¿Se implementan procedimientos apropiados para asegurarse del cumplimiento de estos requisitos?					
33. ¿Se protegen los registros importantes contra pérdidas, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios y contractuales de la empresa Redondos, S.A.?					