UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

METODOLOGÍA PARA LA IMPLEMENTACIÓN, CUMPLIMIENTO Y MEDICIÓN DE UN SGSI A LA MEDIDA DE LA PYME SALVADOREÑA

PARA OPTAR AL GRADO DE

MAESTRO EN SEGURIDAD Y GESTION DE RIESGOS INFORMATICOS

ASESOR:

MAGISTER RENE ANGULO

PRESENTADO POR:

ALEX ANTONIO GUZMÁN MEJÍA

JUAN JOSÉ RIVAS ÁNGEL

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica

Enero de 2016

Contenido

1. Introducción 5
   1.1. La información dentro de las PYMES 5
   1.2. La importancia de la seguridad de la información en las PYMES en El Salvador 6
   1.2.1. Los Sistemas de Gestión de la Seguridad de la Información 6
      1.2.1.1. Cultura de la seguridad de la información 6
   1.2.2. La seguridad de la información en la PYME 10
   1.2.3. El costo de la falta de conocimiento en criterios de seguridad de la información 11
   1.2.4. Marcos de trabajo de la seguridad de la información 14
      1.2.4.1. ITIL 14
      1.2.4.2. COBIT 22
      1.2.4.3. Comparativa de modelos/metodologías de gestión de seguridad y características deseables para un SGSI en las PYMES 29
2. Metodología de trabajo 30
   2.1. Planteamiento del problema 30
   2.2. Hipótesis 31
   2.3. Metodología de la investigación 31
   2.3.1. Objetivos de la investigación 31
   2.3.2. Objetivo general 31
      2.3.2.1. Objetivos específicos 31
   2.3.3. Métodos, técnicas e instrumentos 32
      2.3.3.1. Metodología de la investigación 32
      2.3.3.2. Determinación del objeto de estudio 32
      2.3.3.3. Método 33
      2.3.3.4. Técnicas 34
      2.3.3.5. Instrumento 34
      2.3.3.6. Unidades de análisis y sujetos de estudio 34
      2.3.3.7. Población y muestra 34
      2.3.3.8. Obtención de la muestra 34
      2.3.3.9. Recolección de la información 35
      2.3.3.10. Clasificación, registro y ordenamiento 35
      2.3.3.11. Análisis e interpretación de resultados 35
3. Normalización de la seguridad de la información en El Salvador 121

3.1. Estándar general para la gestión de la seguridad de la información 121
3.1.1. Familia de estándares de la 27000 121
3.1.1.1. ISO/IEC 27000 121
3.1.1.2. ISO/IEC 27001 122
3.1.1.3. ISO/IEC 27002 122
3.1.1.4. ISO/IEC 27003 122
3.1.1.5. ISO/IEC 27004 123
3.1.1.6. ISO/IEC 27005 123
3.1.1.7. ISO/IEC 27006 123
3.1.1.8. ISO/IEC 27007 123
3.1.1.9. ISO/IEC 27008 124
3.1.1.10. ISO/IEC 27009 124
3.1.1.11. ISO/IEC 27010 124
3.1.1.12. ISO/IEC 27011 124
3.1.1.13. ISO/IEC 27012 124
3.1.1.14. ISO/IEC 27013 125
3.1.1.15. ISO/IEC 27014 125
3.1.1.16. ISO/IEC 27015 125
3.1.1.17. ISO/IEC 27016 125
3.1.1.18. ISO/IEC 27017 125
3.1.1.19. ISO/IEC 27018 125
3.1.1.20. ISO/IEC 27019 125
3.1.1.21. ISO/IEC 27031 125
3.1.1.22. ISO/IEC 27032 126
3.1.1.23. ISO/IEC 27033 126
3.1.1.24. ISO/IEC 27034 126
3.1.1.25. ISO/IEC 27035 127
3.1.1.26. ISO/IEC 27036 127
3.1.1.27. ISO/IEC 27037 127
3.1.1.28. ISO/IEC 27038 127
3.1.1.29. ISO/IEC 27039 127
3.1.1.30. ISO/IEC 27040 127
3.1.1.31. ISO/IEC 27041 128

3.1.1.32. ISO/IEC 27042 128
3.1.1.33. ISO/IEC 27043 128
3.1.1.34. ISO/IEC 27044 128
3.1.1.35. ISO/IEC 27799 128
3.2. Adaptación de las 4 normas 128
4. Desarrollo del trabajo 129
4.1. Metodología propuesta 129
Metodología para la implementación, cumplimiento y medición de un SGSI a la medida de la PYME Salvadoreña. 129
0. Introducción 129
1. Alcance 130
2. Referencias normativas 130
3. Términos y definiciones 131
4. Requisitos a cumplir 131
5. Guía de implementación, métricas y mediciones 141
6. Mejora del SGSI 154
Índice de Tablas 158
Índice de figuras 161
Índice de gráficos 162
Bibliografía 164

1. Introducción

La información es uno de los principales activos de las empresas, por esta razón las nuevas tecnologías de la información y la comunicación se han convertido en una herramienta imprescindible para desarrollar cualquier actividad económica, así como un factor clave para mejorar la productividad. En la actualidad, el desarrollo de las nuevas tecnologías ha dado un giro radical a la forma de hacer negocios, a la vez que ha aumentado los riesgos para las empresas que se exponen a nuevas amenazas.

En los últimos años han emergido nuevas formas de ataque que van desde virus informáticos, "phising", robo de información confidencial hasta "ciberterrorismo"; las cuales ponen en riesgo la actividad económica empresarial. Ante este escenario, es importante que las empresas tomen consciencia de la importancia y la urgente necesidad de tomar acción para promover medidas que permitan reducir estos riesgos.

La implementación de medidas o controles debe realizarse de forma ordenada, a través de un proceso sistematizado que permita documentar, normar, medir y mejorar la gestión de la seguridad de la información. Actualmente existen varias metodologías a través de las cuales las empresas pueden alcanzar un grado de madurez aceptable en la Seguridad de la Información.

Un sistema de Gestión de la Seguridad de la Información (SGSI), basado en la norma NTS ISO / IEC 27001:2013, es una herramienta o metodología sencilla y de bajo costo que cualquier Pequeña y Mediana Empresa (PYME) puede utilizar. La norma le permite establecer políticas, procedimientos y controles de seguridad con el objeto de conocer y disminuir los riesgos de su empresa.

1.1. La información dentro de las PYMES

Las empresas son cada vez más dependientes de información para mantener sus actividades empresariales. Por tanto, es lógico pensar que las PYMES que sean capaces de gestionar adecuadamente esta información a través de los sistemas de informáticos, estarán en mejor disposición de alejarse de sus competidores, produciendo mejores ofertas, más competitivas y a la medida de los mercados.

El rumbo de la PYME está orientado por el mercado en el que participe la empresa, las decisiones que se toman para mantener la rentabilidad de la empresa están directamente relacionadas con la calidad de la información que es generada a partir su participación en el mercado. Por tanto, la información es un factor determinante para el proceso de toma de decisiones en la organización.

Una parte muy importante del valor de las PYMES, de la capacidad de suministrar servicio a sus clientes reside en la información, en los datos de sus clientes, en sus productos, en la correspondencia y en muchas más cosas almacenadas en sus computadoras conectadas a internet.

En la actualidad, el mercado se ha conformado cada vez más dinámico, globalizado y exigente en el cual, la PYME debe interrelacionarse tanto a escala nacional como internacional, ante este escenario, la información constituye un componente básico en el desarrollo de este tipo de empresas.

Como ya es conocido, la pérdida de información puede producirse accidental o malintencionadamente, pero, en cualquier caso, produce un daño económico y en la mayoría de ellos afecta la imagen y marca de la empresa. Por lo tanto, la protección y monitorización de cualquier canal electrónico y de la información que circula por ellos es uno de los grandes retos que tiene los profesionales de la Seguridad TI. Para ello, es muy importante tener claro el tipo de información que generan las empresas y de los sistemas que la soporten, realizando una adecuada clasificación de la misma y definiendo medidas de seguridad del manejo de dicha información según la categoría que a la pertenezca.

En las PYMES investigadas, existe una tendencia en considerar como activos de la empresa únicamente los bienes tangibles: mobiliario, maquinaria, equipos, entre otros. No obstante, no debe olvidarse que existen bienes intangibles como la marca de la empresa, el conocimiento comercial, lista de clientes, la propiedad intelectual, entre otros. Todos estos forman parte de la información de la empresa y constituyen uno de los activos más importantes.

El siguiente apartado se centrará en la importancia de la seguridad de la información en las PYMES salvadoreñas, dentro del cual se enumeran temas como la cultura que deben adoptar las empresas y todos sus empleados para proporcionar una mayor seguridad en la información, así mismo, se hará mención de las consecuencias de una mala gestión de la seguridad de la información, mostrando cifras consideradas muy significativas para la economía de las empresas.

1.2. La importancia de la seguridad de la información en las PYMES en El Salvador

1.2.1. Los Sistemas de Gestión de la Seguridad de la Información

1.2.1.1. Cultura de la seguridad de la información

Desplegar una cultura de seguridad de la información en la empresa es uno de los objetivos más complejos de alcanzar. En primer lugar, porque su aplicación requiere de plazos de tiempo extensos y en acciones prolongadas en el tiempo. En segundo lugar, y más importante porque se

trata de personas. Lograr que los equipos de trabajo interioricen en sus tareas diarias una manera de trabajar que asegure que las cosas se hacen bien en materia de seguridad de la información no es una tarea fácil.

Por lo general, los equipos de trabajo ven la implementación de medidas y controles de seguridad como un entorpecimiento o molestia. En muchos casos la percepción es que la seguridad es incómoda y que dificulta sus actividades diarias imponiendo restricciones. Con base en lo anterior, es importante realizar un esfuerzo por revertir la visión negativa y realizar las acciones necesarias para conseguir crear una auténtica cultura de la seguridad dentro de la PYME.

Este esfuerzo requiere la realización de actividades clave que permitan mantener un adecuado nivel de seguridad. A continuación, se presentan algunas:

- Actividades de capacitación y formación para los equipos de trabajo
- Instaurar políticas, regulaciones y procedimientos de seguridad de la información
- Controlar que se cumplen las buenas prácticas en seguridad de la información
- Efectuar acciones de sensibilización y concientización en seguridad para empleados

Figura 1. Cultura de la Seguridad de la Información

Efectuar acciones de sensibilización y concientización en seguridad de la información

Es fundamental que la máxima autoridad se asegure de la implicación de todos sus equipos de trabajo en los aspectos relacionados con la Seguridad de la Información. Estos deben estar

conscientes de la importancia de la información que manejan, tanto la interna como la información de terceros (clientes, proveedores, socios, entre otros). Para conseguir este involucramiento es necesario emprender acciones de formación, sensibilización y concientización necesarias para mantener los niveles de seguridad apropiados.

Si los empleados no se consideran parte fundamental de este proceso, el fracaso está garantizado, ya que ellos son los grandes protagonistas de éste proceso. No sólo porque son los encargados de cumplir las normas y los procedimientos, sino porque también son parte esencial en el mecanismo interno de revisión y mejora proactiva del nivel de seguridad.

Los temas recomendados de capacitación son:

- Uso de correo electrónico
- Gestión de contraseñas
- Uso de dispositivos USB
- Técnicas de ingeniería social
- Navegación segura

El objetivo es que los equipos de trabajo acojan una serie de prácticas sanas en materia de la seguridad, tanto a nivel profesional como personal lo que redundará en una mejora en el nivel de seguridad de la organización.

La formación aumenta el nivel de seguridad en la organización, además de contribuir a mejorar la imagen como empresa ante nuestros clientes y proveedores. Sin duda, estos aspectos inciden positivamente en los procesos comerciales de la empresa.

Actividades de capacitación y formación para los equipos de trabajo

Comúnmente la seguridad de la información en las empresas es entendida como un gasto que no aporta valor al negocio. Si se pregunta por iniciativas relacionadas con la formación en seguridad, en su mayoría veremos que únicamente se tratan de acciones relacionadas con la seguridad en el puesto de trabajo y la prevención de riesgos laborales, dejando fuera la seguridad de la información.

Es fundamental ser conscientes de la importancia de formar a los equipos de trabajo en seguridad de la información, desde el punto de vista de toda la información que trata la empresa: datos de facturación, costos, ventas, sistemas de producción, clientes, proveedores, entre otros.

La seguridad no debe limitarse solamente a aspectos técnicos, sino que debe incorporar otros ámbitos como el organizativo y el legal, traspasando así las competencias del área de sistemas informáticos (en caso que exista).

Instaurar políticas, regulaciones y procedimientos de seguridad

La organización debe asegurarse de contar con los documentos guía que permitan garantizar la instauración de un SGSI. Deberá documentarse cómo se deben hacer las cosas para que no queden al azar y se hagan de la forma establecida y adecuada.

Esto mismo aplica con los diferentes protocolos de actuación de la empresa, que deben ser procedimentados y registrados. De la misma forma debe especificarse lo que se puede y no se puede hacer en la organización, con internet, correo electrónico, entre otros.

Deberá documentarse los procesos sancionatorios a aplicar en caso se dé un uso indebido o incumplimiento a alguna normativa.

Estas normas, regulaciones y procedimientos deben formar parte de la Política de Seguridad de la Información definida en la empresa. La política recoge las intenciones y objetivos de la organización en materia de la seguridad de la información, y su propósito es declarar formalmente que la seguridad es una parte fundamental de la cultura de la empresa. Es por esta razón que los procedimientos, normas y regulaciones que se definan deben ser aprobados por la máxima autoridad en la empresa. Es muy importante que una vez hayan sido aprobados los documentos que rigen la seguridad en la empresa, estos sean comunicados al personal.

Controlar que se cumplen las buenas prácticas en seguridad de la información

Una vez definido el marco de trabajo y comunicado a las áreas interesadas, es indispensable comprobar que efectivamente se está siguiendo y aplicando. Para ello deberá existir un responsable encargado de velar por:

- La vigencia y validez de normas, procedimientos y regulaciones definidos, atendiendo a la detección de nuevas situaciones, de cambios organizativos, prácticas tecnológicas en la organización que recomienden la revisión de los mismos.
- La instauración de los mismos y su cumplimiento por parte de todos los equipos de trabajo.

La comprobación de la implementación de procedimientos y su aplicación se realiza a través de auditorías ya sea internas o externas.

En caso de querer comprobar el uso correcto de los recursos que se ponen a disposición de los equipos de trabajo para el desempeño de sus funciones, es posible implantar diferentes soluciones tecnológicas, que además ayudarán a impedir que se realicen acciones que no están permitidas en las políticas de la empresa.

1.2.2. La seguridad de la información en la PYME

En la actualidad, ante un entorno empresarial globalizado y competitivo, las empresas dependen cada vez más de sus sistemas de información, se ha demostrado que una efectiva gestión de la información tiene una influencia importante para aumentar su nivel de competitividad. Sin embargo, sin una apropiada gestión de la seguridad, la gestión de la información carece de valor, pues no es posible garantizar la confidencialidad, integridad y disponibilidad de la misma.

Generalmente, las PYMES no tienen una visión sobre la situación de su seguridad. La falta de recursos provoca, que muchas PYMES cuenten con una seguridad insuficiente o no sepan las medidas que tiene que adaptar para estar protegidos. A pesar que muchas empresas asumen el riesgo de prescindir de medidas de protección adecuadas, otras muchas han comprendido que la gestión de la información no es posible sin la implementación de un SGSI.

La dinámica de los negocios de El Salvador exige a las PYMES asegurar una posición competitiva, para alcanzar esto es necesario el uso de herramientas tecnológicas tales como: páginas web, correo electrónico, computadoras, dispositivos móviles, entre otros. Todas estas herramientas que permiten realizar operaciones de colaboración requieren el uso de Internet y por tanto deben acompañarse de una gestión que aborde los riesgos que presenta el uso de Internet. Debido a esta situación, hoy en día las empresas están expuestas a una serie de amenazas entre las cuales se pueden mencionar: virus, malware, fuga de información, uso inadecuado de la información, entre otros.

Las PYMES enfrentan un reto importante para abordar la seguridad de manera eficiente a un costo razonable, algunos de estos retos conciernen a las restricciones de presupuesto para la implementación de infraestructura y contratación de personal para atender las amenazas mencionadas, agregando que en la mayoría de los casos investigados las PYMES tienen la percepción que la seguridad no contribuye al crecimiento de la empresa.

Existen en el mercado soluciones de bajo costo, o en muchos casos Software Libre que ofrecen a las empresas soluciones que les permitan obtener una falsa percepción de seguridad, debido a que, si bien implementa controles para mitigar algunos riesgos no brinda una solución integral, es por ello que es necesario que la Dirección se enfoque en la implementación de un marco de trabajo para el gobierno corporativo de IT (según los alcances organizacionales) que permita tener una visión integral de la seguridad de la información, implementando controles de manera más efectiva e integral.

Como se verá a lo largo de este trabajo, actualmente las normativas de seguridad existentes son aplicables principalmente a las grandes empresas debido a los costos o a la falta de formación para su implementación.

1.2.3. El costo de la falta de conocimiento en criterios de seguridad de la información

La dinámica de los negocios en el mundo actual, exige a las empresas de cualquier tamaño y rubro, consolidar una posición competitiva. Para lograr esta posición, son requeridos el uso de herramientas tecnológicas tales como: el correo electrónico, redes sociales, conferencias web, portales electrónicos, cómputo en la nube, dispositivos móviles, portales de pago electrónico, entre otros. Estas herramientas que permiten realizar estas operaciones de negocio tienen un punto en común: requieren de un acceso a Internet. Estos medios de consolidación estratégica deben acompañarse de una gestión que aborde un enfoque de riesgos que contemple los desafíos que hoy en día se presentan en la Internet. Esto es debido a que las empresas se encuentran expuestas a un sinfín de amenazas entre las que se encuentran los delitos cibernéticos, software malicioso (virus y gusanos), fuga de información, uso inadecuado por parte de personal interno y vulnerabilidades de las aplicaciones empresariales por citar algunos.

Normalmente cuando hablamos de ataques informáticos nos enfocamos en grandes empresas u organizaciones gubernamentales, entre otros. La seguridad informática es esencial para sostener los negocios en la actualidad. En este contexto, la falta de seguridad en las PYMES hace que este segmento sea uno de los más “frágiles” en estos términos. Es por esta razón, que en estos días las PYMES se están convirtiendo en un blanco muy atractivo, a causa del aprovechamiento que se está dando por la poca seguridad con que se cuenta en este tipo de empresas, el cual, uno de los principales objetivos de ataque pudiera ser, por ejemplo, la adquisición de la información de secretos industriales y así demorar los planes de competencia. Uno de los principales blancos dentro de estas empresas, pueden estar relacionados con las Bases de Datos, la información de clientes, los procesos, etc. Es importante aclarar que como los delitos evolucionan constantemente, no existe un sistema preciso para controlar ese tipo de acciones. Por esto, es que es necesario trabajar de manera constante y de modo preventivo y no reactivo. Además, los ataques suelen suceder de igual manera, tanto desde adentro de las propias empresas como desde afuera.

En relación con el costo de tener una empresa protegida, éste depende del tamaño de la empresa y el diseño específico que se desea y, sobre todo, de la cultura organizacional. En ese sentido, las

grandes compañías tienen ventajas porque cuentan con áreas específicas, mientras que las PYMES suelen actuar reactivamente. Aun cuando sean conscientes los riesgos asumidos, muchas organizaciones consideran difícilmente justificable el esfuerzo que requiere mantener la seguridad. Y si a esto le unimos la grave escasez de profesionales en materia de seguridad, lo que consecuentemente produce que las compañías perciban la seguridad como un alto costo que debe de justificarse lo suficientemente bien para ser aprobado.

Existen cifras que muestran la magnitud de los problemas ocasionados por la falta de medidas de seguridad, por ejemplo, el 31% de las PYMES en Latinoamérica reconocieron haber sufrido al menos un ciberataque en el 2010. Mientras que el 70% de las compañías ve como un factor de riesgo para su negocio los temas informáticos y la fuga de información[1].

Países en estudio: Argentina, Colombia, México, entre otros.	**Porcentaje**
Presupuesto de las PYMEs para seguridad de la información	8%
Empresas PYME que sufrieron un ataque informático	73%

Tabla 1. Las PYMES se están preocupando por su seguridad informática.

"McAffe ha realizado un estudio en diferentes países como Argentina, Colombia, México, entre otros, cuya finalidad era identificar los gastos en tecnología por tamaño de las empresas en Latinoamérica, Según McAfee, solo el 8% del gasto en TI de las pequeñas y medianas empresas está destinado a la seguridad informática. Teniendo en cuenta que el 73% de las Pymes colombianas sufrieron por lo menos un ataque informático, y que estas compañías mueven el 96% de la economía del país, es preocupante la falta de aseguramiento informático. Por otro lado, se registró un total de más de 37 millones de dólares, de los cuales 36,3% fueron de PYMES, lo que indica la importancia que están tomando las PYMES en materia de seguridad de la información. Este estudio revelo también, que actualmente las PYMES se han comenzado a preocupar por obtener o generar estrategias que permitan fortalecer la seguridad de su información, y al estar conscientes de los riesgos que se exponen, en el 2010 las PYMES invirtieron mundialmente $9.470.000.000 de dólares en seguridad" [2].

[1] *(2012). Las pymes se están preocupando por su seguridad informática. Recuperado de: http://actualicese.com/actualidad*

[2] *Santos, M.(2013). Los retos de seguridad para las PYMES. Bogota, Colombia. ETB,Enter.co. Recuperado de: http://www.enter.co*

Por otra parte, un estudio de Applied Research, desarrolladora de aplicaciones de software financiero, realizado en empresas de Brasil, México, Argentina y Colombia, identificó los mayores riesgos para el negocio. En este sentido, además del terrorismo, los desastres naturales y la actividad criminal, en Latinoamérica el 70% de las compañías ve como un factor de riesgo para su negocio los temas informáticos y la fuga de información.

"En otros estudios, ante los riesgos informáticos las PYMES necesitan tomar precauciones para evitar sorpresas de ataques externos. Según Coelco (Comercio electrónico del conocimiento), un 50% de los delitos a futuro se cometerán por medio de sistemas virtuales (ciberfraudes), resaltando que un 50% de las pymes nacionales no aplican una política de seguridad informática.

Por otro lado, Panda Security entrega un dato importante, el 64% de las PYMES han sido sobrepasadas por la seguridad informática, de las cuales en un 47% de las veces han visto afectada su productividad, a pesar que un 97% tenga instalado un programa antivirus. Uno de los motivos de esta situación es no observar los procesos críticos ni detectar la amenaza.

Como consecuencia de lo anterior, contar con medidas como software específico o un especialista para mantener los equipos más que un lujo es una necesidad. En España el gasto en seguridad en las pymes con respecto al año anterior se ha mantenido en un 61% de las empresas, mientras que en un 10% a disminuido, y en un 2% ha subido sustancialmente"[3].

Criterios de seguridad de la información	Niveles de Porcentaje	
	McAfee/Latinoamérica	Panda Security / España
Inversión en la seguridad informática	8%	61%
Registro de ataques informáticos	73%	64%
Importancia de la seguridad	36%	-
Afectación de productividad en las empresas	-	47%

Tabla 2. Criterios de seguridad de la información según estudios realizados en el año 2010 por McAfee y Panda Security

[3] *BAQUIA. (2009). Seguridad informática para pymes: ¿Gasto o inversión? Madrid, España. Recuperado de: http://www.baquia.com*

1.2.4. Marcos de trabajo de la seguridad de la información

1.2.4.1. ITIL

ITIL es un marco de trabajo público que propone un conjunto de mejores prácticas de TI para la Gestión de Servicios. Proporciona un marco para el gobierno de TI y se enfoca en la medición y mejora constante de la calidad del servicio entregado, considerando la perspectiva del negocio y cliente.

ITIL permite beneficiarse completamente de las mejores prácticas demostradas en TI y es relevante para cualquier persona encargada de la entrega o apoyo de servicios de TI.

ITIL se alinea con varias normas de calidad internacionales, incluyendo ISO/IEC 20000 (Código de Prácticas de la Gestión de Servicios de TI) y ha sido aceptado por miles de organizaciones de todo el mundo tales como la NASA, el Servicio de Salud del Reino Unido, entre otros.

Algunos beneficios que ofrece este modelo de gestión son:

- Incremento de la satisfacción de clientes y usuarios con los servicios de TI
- Reducción de tiempo para el lanzamiento de nuevos servicios asegurando la satisfacción del cliente
- Control y reducción de costos
- Mejora de la toma de decisiones
- Florecimiento en la administración de riesgos
- Mejorar la integración de TI con el negocio
- Optimiza las líneas de comunicación
- Mejora de la calidad del servicio
- Contar con un modelo de gobernabilidad
- Mejorar la Gestión de Proveedores

Algunas características de este marco de trabajo:

- Es aplicable para cualquier organización que maneje TI, no se basa en una tecnología y no depende de ninguna para su funcionamiento.
- No prescribe
- No es una fórmula para todas las organizaciones, pueden ser adaptadas en tiempo y alcance de acuerdo a las necesidades.

ITIL establece que el servicio es un medio para entregar valor a los clientes facilitando resultados que los clientes quieren lograr sin asumir los costos y riesgos específicos requeridos para obtener el producto (servicio).

Un servicio de TI, está conformado por una combinación de tecnología, personas y procesos. Es provisto por un proveedor de servicios de TI.

A continuación, se detallan los tipos de servicios según ITIL:

- Servicios principales: aquellos que entregan los resultados deseados a los clientes
- Servicios habilitadores, son aquellos que se necesitan para entregar un servicio principal.
- Servicios mejorados, son aquellos que son añadidos a los servicios principales con el propósito de mejorar la experiencia para el cliente.

Otro concepto importante, es el "paquete de servicios", el cual se define como una colección de servicios que han sido combinados para ofrecer una solución específica a un tipo de necesidad.

La Gestión del Servicio

Es un set de capacidades organizacionales especializadas para la provisión de valor a los clientes en forma de servicios.

Puede entenderse también, como el acto de transformar las capacidades y recursos en servicios de valor, lo que permitirá a la organización alcanzar sus resultados.

Para llevar a cabo la Gestión del Servicio, debe comprenderse como el negocio ve la organización de TI:

- TI es una colección de sistemas, aplicaciones e infraestructuras que son componentes de un producto.
- TI es una organización que tiene capacidades y recursos.
- TI es una categoría de servicios, utilizados por el negocio.
- TI es una categoría de activos de negocio, que provee beneficios a sus propietarios que incluyen ingresos y ganancias.

La Gestión de los Servicios de TI es desempeñada por un proveedor en una apropiada combinación de personas, procesos y tecnología.

El Valor del Servicio, es considerado como el nivel que un servicio alcanza las expectativas de un cliente. Es determinado por el cliente y no por el proveedor del servicio, ya que ellos (los clientes) deciden que cual será la utilidad del servicio y el tipo de retorno que alcanzarán por su uso.

El valor de un servicio es creado por la combinación de 2 elementos primarios:

- Utilidad, es la funcionalidad ofrecida por un producto para alcanzar una necesidad en particular.
- Garantía, se refiere a la habilidad del servicio para estar disponible cuando se necesite, para proveer la capacidad requerida y proveer fiabilidad en términos de continuidad y seguridad.

El ciclo de vida del Servicio en ITIL presenta la aproximación para la Gestión del Servicio, por medio de un marco de trabajo llamado Ciclo de Vida del Servicio, que representa los estados o fases de un servicio durante su vida:

- Estrategia del Servicio

  Provee una guía para visualizar la gestión de servicio como un activo estratégico y no únicamente como una capacidad organizacional. La creación de valor comienza con el entendimiento de los objetivos organizacionales y de las necesidades del cliente.

- Diseño del Servicio

  Provee una guía para el diseño y desarrollo de los servicios y gestión del servicio con los objetivos del negocio en mente. El diseño del servicio no está limitado a los nuevos servicios, incluyen también los cambios y mejoras necesarias para incrementar o mantener el valor para los clientes, a lo largo del ciclo de vida del servicio.

- Transición del Servicio

  Ofrece una guía para la introducción de servicios nuevos o cambiados en ambientes de producción, controlando el riesgo y proporcionando el conocimiento necesario para la toma de decisiones.

- Operación del Servicio

  Describe las mejores prácticas para el manejo de servicios en ambientes productivos.

- Mejora continua del Servicio

  Ofrece una guía para la creación y mantenimiento del valor para los clientes, a través de una mejora estrategia, diseño, transición y operación del servicio. Combina principios, prácticas y métodos de gestión de calidad, gestión de cambio y mejora de capacidades.

La estructura del ciclo de vida de un Servicio debe estar soportada por una estructura organizacional, el portafolio de servicios y un modelo de servicios dentro de una organización.

ITIL Gestión de la Seguridad de TI

Objetivo: Asegurar la confidencialidad, la integridad y la disponibilidad de la información, datos y servicios de TI de una organización. Por lo general, la Gestión de Seguridad de TI forma parte del acercamiento de una organización a la gestión de seguridad, cuyo alcance es más que el del proveedor de Servicios de TI.

Definición del proceso:

ITIL V3 2011 clasifica la Gestión de la Seguridad de la Información de TI en el proceso de Diseño del Servicio logrando así una mejor integración dentro del Ciclo de Vida del Servicio.

Subprocesos:

- Diseño de controles de seguridad:
  Objetivo procesal: Diseñar técnicas y medidas organizativas adecuadas que aseguren la confidencialidad, disponibilidad e integridad de los activos de información de una organización.
- Pruebas de Seguridad:
  Objetivo procesal: Asegurar que todos los mecanismos y controles de seguridad sean objeto de pruebas y revisiones frecuentes.
- Gestión de incidentes de seguridad:
  Objetivo: Detectar y combatir ataques e intrusiones y minimizar los daños causados por actos contra la seguridad
- Revisión de seguridad
  Objetivo procesal: Revisar que las medidas y procedimientos de seguridad sean acordes a con la percepción de riesgos en la empresa, y verificar que esas medidas y procedimientos sean sometidas a prueba y reciban mantenimiento frecuente.

Objetivos de la Gestión de la Seguridad:

- Diseñar una política de seguridad, en colaboración con clientes y proveedores correctamente alineada con las necesidades del negocio.
- Asegurar el cumplimiento de los estándares de seguridad acordados
- Minimizar los riesgos de seguridad que amenacen la continuidad del servicio

La Gestión de la seguridad debe conocer en profundidad el negocio y los servicios que presta la organización TI para establecer protocolos de seguridad que aseguren que la información esté accesible cuando se necesita por aquellos que tengan autorización para utilizarla.

Una vez comprendidos cuales son los requisitos de seguridad del negocio, la Gestión de la Seguridad debe supervisar que estos se hallen convenientemente plasmados en los Acuerdos de Nivel de Servicio (SLA por sus siglas en inglés) correspondientes para garantizar su cumplimiento.

Los principales beneficios de una correcta Gestión de la Seguridad:

- Se evitan interrupciones del servicio causadas por virus, ataques informáticos, entre otros.

- Se minimiza el número de incidentes.
- Se tiene acceso a la información cuando se necesita y se preserva la integridad de los datos.
- Se preserva la confidencialidad de los datos y la privacidad de clientes y usuarios.
- Se cumplen los reglamentos sobre protección de datos.
- Mejora la percepción y confianza de clientes y usuarios en lo que respecta a la calidad del servicio.

Las principales dificultades a la hora de implementar la Gestión de la Seguridad se resumen en:

- No existe el suficiente compromiso de todos los miembros de la organización TI con el proceso.
- Se establecen políticas de seguridad excesivamente restrictivas que afectan negativamente al negocio.
- No se dispone de las herramientas necesarias para monitorizar y garantizar la seguridad del servicio (firewalls, antivirus, ...).
- El personal no recibe una formación adecuada para la aplicación de los protocolos de seguridad.
- Falta de coordinación entre los diferentes procesos lo que impide una correcta evaluación de los riesgos.

Proceso:

La Gestión de la Seguridad está estrechamente relacionada con prácticamente todos los otros procesos TI y necesita para su éxito la colaboración de toda la organización.

Para que esa colaboración sea eficaz es necesario que la Gestión de la Seguridad:

- Establezca una clara y definida política de seguridad que sirva de guía a todos los otros procesos.
- Elabore un Plan de Seguridad que incluya los niveles de seguridad adecuados tanto en los servicios prestados a los clientes como en los acuerdos de servicio firmados con proveedores internos y externos.
- Implemente el Plan de Seguridad.
- Monitorice y evalúe el cumplimiento de dicho plan.
- Supervise proactivamente los niveles de seguridad analizando tendencias, nuevos riesgos y vulnerabilidades.

- Realice periódicamente auditorías de seguridad.

Política de Seguridad:

En particular la Política de Seguridad debe determinar:

- La relación con la política general del negocio.
- La coordinación con los otros procesos TI.
- Los protocolos de acceso a la información.
- Los procedimientos de análisis de riesgos.
- Los programas de formación.
- El nivel de monitorización de la seguridad.
- Qué informes deben ser emitidos periódicamente.
- El alcance del Plan de Seguridad.
- La estructura y responsables del proceso de Gestión de la Seguridad.
- Los procesos y procedimientos empleados.
- Los responsables de cada subproceso.
- Los auditores externos e internos de seguridad.
- Los recursos necesarios: software, hardware y personal.

Plan de seguridad:

El objetivo del Plan de Seguridad es fijar los niveles de seguridad que han de ser incluidos como parte de los Acuerdos de Nivel de Servicio (por sus siglas en ingles SLA) y Acuerdo de Nivel de Operación (por sus siglas en ingles OLA) y Contratos de Soporte con proveedor externo (por sus siglas en ingles UC).

Este plan ha de ser desarrollado en colaboración con la Gestión de Niveles de Servicio que es la responsable en última instancia tanto de la calidad del servicio prestado a los clientes como la del servicio recibido por la propia organización de TI y los proveedores externos.

El Plan de Seguridad debe diseñarse para ofrecer un mejor y más seguro servicio al cliente y nunca como un obstáculo para el desarrollo de sus actividades de negocio.

Siempre que sea posible deben definirse métricas e indicadores clave que permitan evaluar los niveles de seguridad acordados.

Un aspecto esencial a tener en cuenta es el establecimiento de unos protocolos de seguridad coherentes en todas las fases del servicio y para todos los estamentos implicados.

Aplicaciones de las medidas de seguridad:

Es responsabilidad de la Gestión de Seguridad coordinar la implementación de los protocolos y medidas de seguridad establecidas en la Política y el Plan de Seguridad.

En primer lugar, la Gestión de la Seguridad debe verificar que:

- El personal conoce y acepta las medidas de seguridad establecidas, así como sus responsabilidades al respecto.
- Los empleados firmen los acuerdos de confidencialidad correspondientes a su cargo y responsabilidad.
- Se imparte la formación pertinente.

Es también responsabilidad directa de la Gestión de la Seguridad:

- Asignar los recursos necesarios.
- Generar la documentación de referencia necesaria.
- Colaborar con el Service Desk y la Gestión de Incidentes en el tratamiento y resolución de incidentes relacionados con la seguridad.
- Instalar y mantener las herramientas de hardware y software necesarias para garantizar la seguridad.
- Colaborar con la Gestión de Cambios y Versiones para asegurar que no se introducen nuevas vulnerabilidades en los sistemas en producción o entornos de pruebas.
- Proponer RFCs a la Gestión de Cambios que aumenten los niveles de seguridad.
- Colaborar con la Gestión de la Continuidad del Servicio para asegurar que no peligra la integridad y confidencialidad de los datos en caso de desastre.
- Establecer las políticas y protocolos de acceso a la información.
- Monitorizar las redes y servicios en red para detectar intrusiones y ataques.

Es necesario que la gestión de la empresa reconozca la autoridad de la Gestión de la Seguridad respecto a todas estas cuestiones y que incluso permita que ésta proponga medidas disciplinarias vinculantes cuando los empleados u otro personal relacionado con la seguridad de los servicios incumplan con sus responsabilidades.

Evaluación y Mantenimiento

Evaluación:

Aunque no es imprescindible, es recomendable que estas evaluaciones se complementen con auditorías de seguridad externas y/o internas realizadas por personal independiente de la Gestión de la Seguridad.

Estas evaluaciones/auditorias deben valorar el rendimiento del proceso y proponer mejoras que se plasmarán en las Solicitudes de Cambio (por sus siglas en inglés RFC) que habrán de ser evaluados por la Gestión de Cambios.

Independientemente de estas evaluaciones de carácter periódico se deberán generar informes independientes cada vez que ocurra algún incidente grave relacionado con la seguridad. De nuevo, si la Gestión de la Seguridad lo considera oportuno, estos informes se acompañarán de las RFCs correspondientes.

Mantenimiento:

La Gestión de la Seguridad es un proceso continuo y se han de mantener al día el Plan de Seguridad y las secciones de seguridad de los SLAs.

Los cambios en el Plan de Seguridad y los SLAs pueden ser resultado de la evaluación / auditoría o de cambios implementados en la infraestructura o servicios TI.

Es así mismo importante que la Gestión de la Seguridad esté al día en lo que respecta a nuevos riesgos y vulnerabilidades frente a virus, spyware, ataques de denegación de servicio, etcétera, y que adopte las medidas necesarias de actualización de equipos de hardware y software, sin olvidar el apartado de formación.

Control del proceso:

Al igual que en el resto de procesos TI es necesario realizar un riguroso control del proceso para asegurar que la Gestión de la Seguridad cumple sus objetivos.

Una buena Gestión de la Seguridad debe traducirse en una:

- Disminución del número de incidentes relacionados con la seguridad.
- Un acceso eficiente a la información por el personal autorizado.

- Gestión proactiva que permita identificar vulnerabilidades potenciales antes de que estas se manifiesten y provoquen una seria degradación de la calidad del servicio.

La correcta elaboración de informes permite evaluar el rendimiento de la Gestión de Seguridad y aporta información de vital importancia a otras áreas de la infraestructura TI.

Entre la documentación generada cabría destacar:

- Informes sobre el cumplimiento, en lo todo lo referente al apartado de seguridad, de los SLAs, OLAs y UCs en vigor.
- Relación de incidentes relacionados con la seguridad calificada por su impacto sobre la calidad del servicio.
- Evaluación de los programas de formación impartidos y sus resultados.
- Identificación de nuevos peligros y vulnerabilidades a las que se enfrenta la infraestructura TI.
- Auditorías de seguridad.
- Informes sobre el grado de implementación y cumplimiento de los planes de seguridad establecidos.

1.2.4.2. COBIT

Los Objetivos de Control para la Información y las Tecnologías Relacionadas (COBIT), ayuda a satisfacer las múltiples necesidades de la administración, estableciendo un puente entre los riesgos del negocio, controles necesarios y los aspectos técnicos. Provee las buenas prácticas a través de los dominios y el marco referencial de los procesos y presenta actividades en una estructura manejable y lógica.

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.

Figura 2. Principios de COBIT

Cobit 5 se basa en cinco principios clave mostrados en la figura 1, para el gobierno y la gestión de las TI empresariales:

Principio 1. Satisfacer las necesidades de las partes interesadas.

Las empresas existen para crear valor para sus accionistas. En consecuencia, cualquier empresa, comercial o no. Tendrá la creación de valor como un objetivo de Gobierno. Creación de valor significa conseguir beneficios a un costo óptimo de los recursos mientras se optimiza el riesgo. (Ver figura 2.) Los beneficios pueden tomar muchas formas, por ejemplo, financieros para las empresas comerciales o de servicio público para entidades gubernamentales.

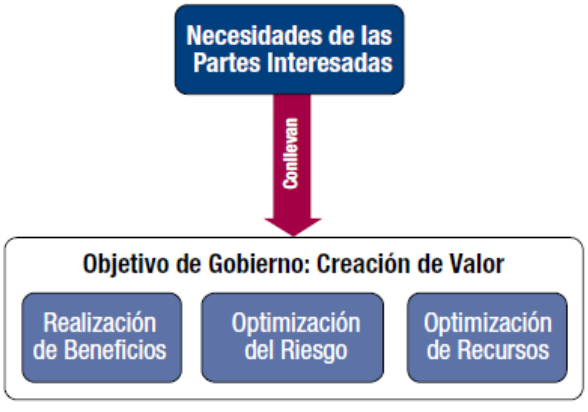

Figura 3. El objetivo de Gobierno: Creación de Valor

Principio 2. Cubrir la empresa extremo a extremo

COBIT contempla el gobierno y la gestión de la información y la tecnología relacionada desde una perspectiva extremo a extremo y para toda la empresa, esto significa que COBIT:

- Integra el gobierno de la empresa TI en el gobierno corporativo. Es decir, el sistema de gobierno para le empresa TI propuesto por COBIT se integra sin problemas en cualquier sistema de gobierno. COBIT se alinea con las últimas visiones sobre gobierno.
- Cubre todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas donde quiera que esa información pueda ser procesada. Dado éste alcance corporativo amplio, COBIT contempla todos los servicios TI internos y externos relevantes, así como los procesos de negocio internos y externos.

COBIT proporciona una visión integral y sistémica del gobierno y la gestión de la empresa TI basada en varios catalizadores. Los catalizadores son para toda la empresa y extremo a extremo, es decir, incluyendo todo y a todos, internos y externos, que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionada, incluyendo las actividades y responsabilidades tanto de las funciones Ti como las funciones de negocio.

El enfoque de gobierno extremo a extremo que es la base de COBIT está representado en la figura 3, mostrando los componentes clave de un sistema de gobierno.

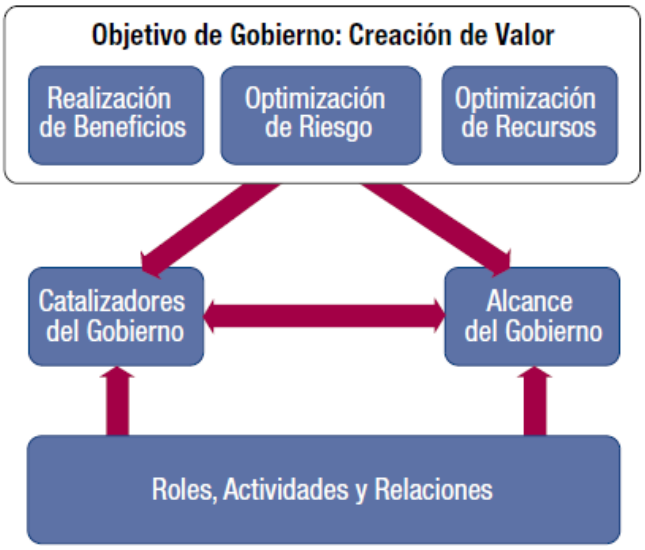

Figura 4. Gobierno y Gestión en COBIT

Principio 3. Aplicar un marco de referencia único e integrado

COBIT es un marco de referencia único e integrado porque:

- Se alinea con otros estándares y marcos de referencia relevantes y, por tanto, permite a la empresa usar COBIT como el marco integrador general de gestión y gobierno.
- Es completo en cuanto a la cobertura de la empresa, proporcionando una base para integrar de manera efectiva otros marcos, estándares y prácticas utilizadas. Un marco general único sirve como fuente consistente e integrada de guía en un lenguaje común, no-tecnico y tecnológicamente agnóstico.
- Proporciona una arquitectura simple para estructurar los materiales de guía y producir un conjunto consistente
- Integra todo el conocimiento disperso previamente en los diferentes marcos de ISACA

4. Hacer posible un enfoque holístico

Los catalizadores son factores que, individual y colectivamente, influyen sobre si algo funcionará en este caso, el gobierno y la gestión de la empresa TI. Los catalizadores son guiados por la cascada de metas, es decir, objetivos de alto nivel relacionados con TI definen lo que los diferentes catalizadores deberían conseguir.

Principio 5. Separar el gobierno de la gestión

El marco de COBIT 5 realiza una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren estructuras organizativas diferentes y sirven para diferentes propósitos. La posición de COBIT 5 sobre esta fundamental distinción entre gobierno y gestión es:

- Gobierno: El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

En la mayoría de las empresas, el gobierno es responsabilidad del consejo de administración bajo la dirección de su presidente.

- Gestión: La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

En la mayoría de las empresas, la gestión es responsabilidad de la dirección ejecutiva bajo la dirección del CEO.

La figura 4 muestra el conjunto completo de los 37 procesos de gobierno y gestión de COBIT 5. Los detalles de todos los procesos, de acuerdo con el modelo de proceso anteriormente descrito, están recogidos en la guía COBIT: Procesos Catalizadores.

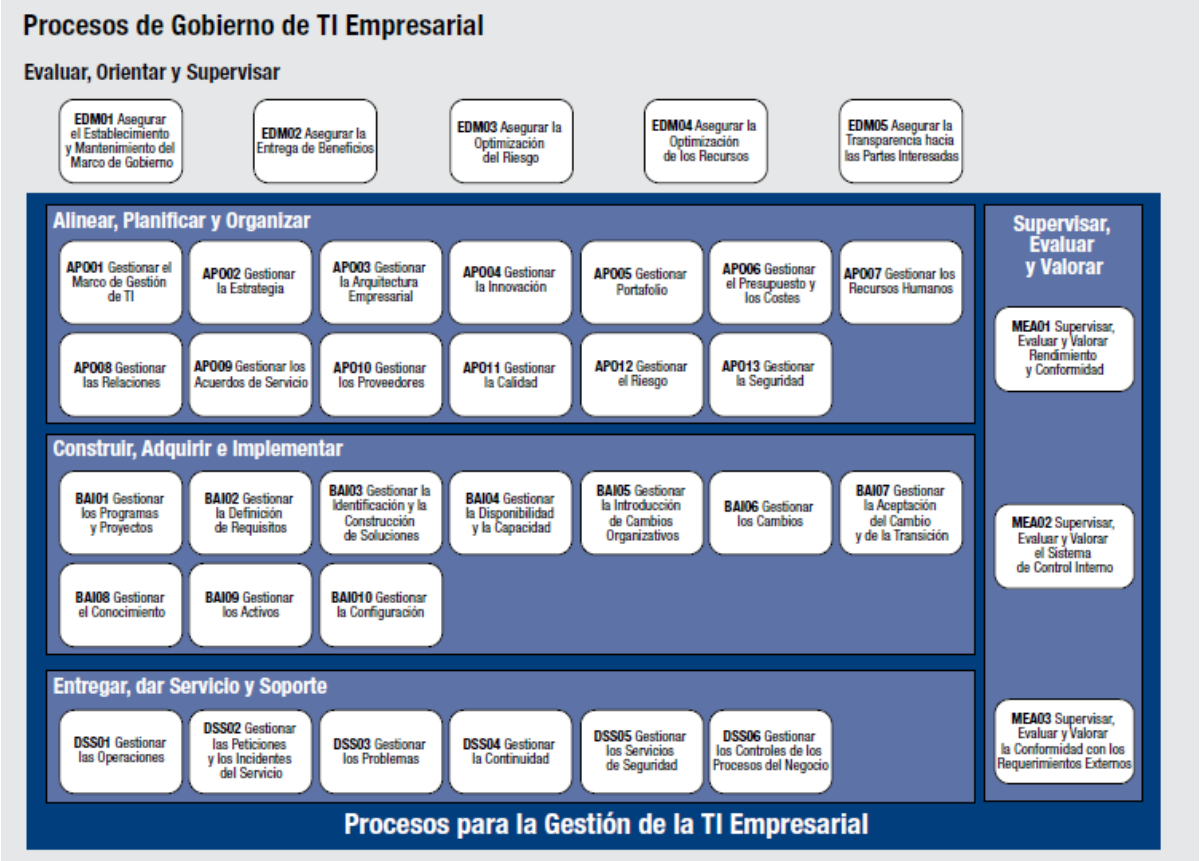

Figura 5. Modelo de referencia de procesos de COBIT 5.

Ciclo de vida

La implementación del ciclo de vida proporciona a las empresas una manera de usar COBIT para solucionar la complejidad y los desafíos que normalmente aparecen durante las implementaciones. Los tres componentes interrelacionados del ciclo de vida son:

1. Ciclo de vida de Mejora continua – Este no es un proyecto único.
2. Habilitación del cambio – Abordar los aspectos culturales y de comportamiento.
3. Gestión del programa.

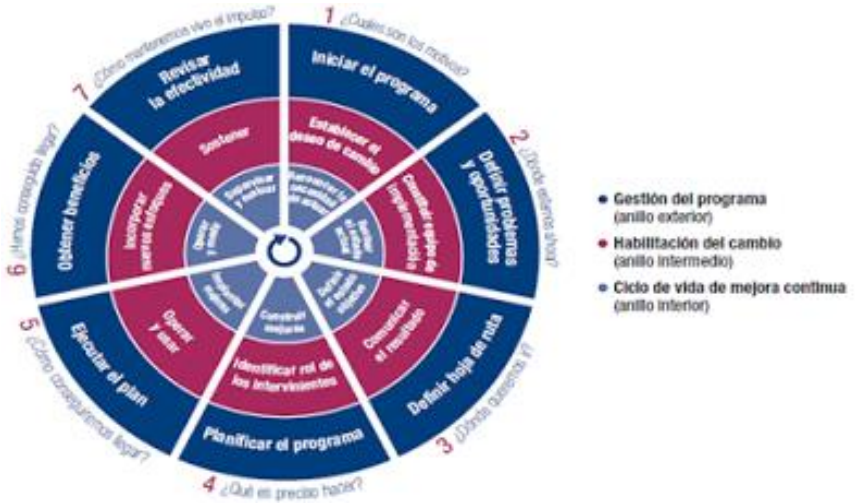

Figura 6. Las siete fases de la implementación del ciclo de vida

La fase 1 comienza con el reconocimiento y aceptación de la necesidad de una iniciativa de implementación o mejora.

Identifica los puntos débiles actuales y desencadena y crea el ánimo de cambio a un nivel de dirección ejecutiva.

La fase 2 se concentra en definir el alcance de la iniciativa de implementación o mejora empleando el mapeo de COBIT de metas empresariales con metas de TI a los procesos de TI asociados, y considerando cómo los escenarios de riesgos podrían destacar los procesos clave en los que focalizarse. Los diagnósticos de alto nivel también pueden ser útiles para delimitar y entender áreas de alta prioridad en las que hacer foco. Se lleva a cabo una evaluación del estado actual y se identifican los problemas y deficiencias mediante la ejecución de un proceso de revisión de capacidad. Se deberían estructurar iniciativas de gran escala como múltiples iteraciones del ciclo de vida para cada iniciativa de implementación que exceda de seis meses, existe un riesgo de perder el impulso, el foco y la involucración de las partes interesadas.

Durante la fase 3, se establece un objetivo de mejora, seguido de un análisis más detallado aprovechando las directrices de COBIT para identificar diferencias y posibles soluciones. Algunas soluciones pueden ser beneficios inmediatos (quick wins) y otras actividades pueden ser más desafiantes y de largo plazo. La prioridad deberían ser aquellas iniciativas que son más fáciles de conseguir y aquellas que podrían proporcionar los mayores beneficios.

La fase 4 planifica soluciones prácticas mediante la definición de proyectos apoyados por casos de negocios justificados.

Además, se desarrolla un plan de cambios para la implementación. Un caso de negocio bien desarrollado ayuda a asegurar que se identifican y supervisan los beneficios del proyecto.

Las soluciones propuestas son implementadas en prácticas día a día en la fase 5. Se pueden definir las mediciones y establecer la supervisión empleando las metas y métricas de COBIT para asegurar que se consigue y mantiene la alineación con el negocio y que el rendimiento puede ser medido. El éxito requiere el compromiso y la decidida apuesta de la alta dirección, así como la propiedad por las partes afectadas a nivel TI y de negocio.

La fase 6 se focaliza en la operación sostenible de los nuevos o mejorados catalizadores y de la supervisión de la consecución de los beneficios esperados.

Durante la fase 7, se revisa el éxito global de la iniciativa, se identifican requisitos adicionales para el gobierno o la gestión de la TI empresarial y se refuerza la necesidad de mejora continua.

COBIT y la gestión de la seguridad

El proceso APO13 de COBIT 5 requiere que un SGSI sea desarrollado e implementado para coordinar y gestionar de forma eficaz y eficiente los recursos y los procesos utilizados, y los controles necesarios para garantizar la confidencialidad, integridad y disponibilidad de los sistemas de información.

El proceso APO13 (gestión de seguridad de la información) se ocupa de una amplia gama de temas y de los activos que respaldan las operaciones del negocio. Apenas hay una actividad de TI que no está vinculada a la seguridad de la información. En COBIT 5 cada proceso tiene un aspecto que seguridad de la información impactos o se ve afectada por la seguridad de la información.

Debido a que la necesidad es ubicua, seguridad de la información se maneja mejor con un solo sistema de gestión integral. Esto es similar a la norma ISO 27001, que también requiere de un conjunto de elementos interrelacionados o que interactúan, que las organizaciones utilizan para dirigir y controlar cómo se implementan las políticas de seguridad y se logran los objetivos de seguridad. Al igual que con el sistema de gestión de COBIT 5 APO13 de seguridad de la información, el propósito del sistema de gestión ISO 27001 es orquestar y coordinar las diversas acciones que se requieren para diseñar, implementar, ejecutar y mantener el nivel deseado de seguridad de la información en toda la organización.

1.2.4.3. Comparativa de modelos/metodologías de gestión de seguridad y características deseables para un SGSI en las PYMES

A continuación, se presenta una comparativa de los diferentes modelos / metodologías de gestión de seguridad de la información y las características deseables para un SGSI en las PYMES.

	Aspectos Analizados									
Modelos/Metodologias de Gestion de Seguridad de la Informacion	**Ciclo de SGSI**	**Marco de Trabajo**	**Nivel de Madurez**	**Cultura de Seguridad**	**Guia de buenas practicas**	**Analisis de riesgos**	**Metricas**	**Orientado a PYMES**	**Reutiliza el conocimiento**	**Casos practicos**
NTS ISO/IEC 27001:2013	Si	Si	Si	Parc	Si	Si	Parc	No	No	Si
ITIL	Si	Si	No	No	No	No	No	No	No	Si
COBIT	Si	Si	No	Parc	Si	Si	Si	No	No	Si
METODOLOGIA PROPUESTA - PYME	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si

Tabla 3. Modelos/metodologías de gestión de seguridad

En la Tabla 1 se puede observar una comparativa de los diferentes modelos y/o metodologías analizadas en esta sección para gestionar la seguridad, incluyendo la metodología desarrollada, con las características deseables para las PYMES de El Salvador. Se considera que los aspectos valorados se pueden cumplir de forma total, parcialmente o no haber sido abordados en el modelo. A continuación, se describen cada uno de los aspectos analizados:

- Ciclo de SGSI: El modelo describe de forma clara las fases de desarrollo, implementación y mantenimiento del SGSI. Normalmente los modelos utilizan el ciclo PDCA.
- Marco de Trabajo: El modelo describe de forma clara todos los elementos que forman el SGSI una vez ha sido implantado.
- Niveles de madurez: El modelo está orientado a la implantación de una seguridad progresiva basada en niveles.
- Cultura de seguridad: El modelo ha tenido en cuenta la orientación hacia la cultura de la seguridad y no solo la orientación técnica y de gestión de los modelos clásicos.
- Guía de buenas prácticas: El modelo incluye una guía de buenas prácticas o controles para la seguridad.
- Análisis y gestión del riesgo: El modelo incluye métodos de valoración y gestión de los riesgos de los sistemas de información

- Métricas: Incluye mecanismos para la medición del cumplimiento de los controles de seguridad.
- Orientado a PYMES: El modelo es orientado para las particularidades de las PYMES.
- Reutiliza el conocimiento: El modelo adquiere el conocimiento de implantaciones ya realizadas para luego ser reutilizadas para implantaciones posteriores.
- Dispone de herramienta software: Dispone de una herramienta que lo soporte.
- Casos prácticos: El modelo ha sido diseñado a partir de observaciones directas y casos prácticos.

2. Metodología de trabajo

2.1. Planteamiento del problema

La información es uno de los activos más importantes de toda organización, por lo que debe ser protegida convenientemente frente a amenazas que pueden poner en peligro la continuidad de los niveles de competitividad, rentabilidad y conformidad legal necesarios para alcanzar los objetivos de la empresa.

Actualmente la mayor parte de información reside en equipos informáticos, redes de datos y soportes de almacenamiento, encuadrados todos dentro de lo que se conoce como sistemas de información. Estos sistemas de información están sujetos a riesgos e inseguridades tanto desde dentro de la organización como desde fuera.

En nuestro país, la PYME no está al margen de esta problemática, la mayor parte de las empresas del sector carecen de orientación adecuada sobre las medidas y controles de seguridad de la información que deben implementar para proteger apropiadamente los sistemas de información. En ese sentido, es importante que los directivos conozcan sobre el estado actual de sus empresas con respecto a los riesgos a los que están expuestos y las acciones que deben tomar para gestionar de manera efectiva la seguridad de la información.

"Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia

organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos. (Normalización, 2015)*"* [4]

Ante este escenario, surge la necesidad de desarrollar un documento basado en las normas de la familia 27000 y adaptado al contexto de la PYME, con el objetivo de hacer posible la prevención o reducción de forma eficaz del nivel de riesgo, a través de la implantación de controles adecuados para preparar a la organización a actuar ante posibles emergencias y garantizar la continuidad del negocio.

2.2. Hipótesis

En El Salvador las pequeñas y medianas empresas carecen de una visión global de los aspectos básicos de la seguridad de la información. La falta de recursos económicos y la falta de conocimientos técnicos provocan que gran parte de las PYMES cuenten con seguridad insuficiente y desconozcan sobre las medidas que deben adaptar para estar protegidos.

2.3. Metodología de la investigación

2.3.1. Objetivos de la investigación

2.3.2. Objetivo general

Obtener información mediante una investigación de campo, sobre el nivel de madurez de un SGSI en las PYMES de El Salvador, información que oriente a la elaboración de una metodología estratégica para la implementación del mismo.

2.3.2.1. Objetivos específicos

- Obtener un diagnóstico sobre el nivel de gestión de la seguridad de la información que dé a conocer las debilidades y necesidades.
- Disponer de un marco corporativo, bajo un estándar internacional, que regule todos los aspectos relativos a la seguridad de la información.
- Diseñar una metodología para la implantación de un SGSI para PYMES
- Presentar criterios de buenas prácticas para la PYME de El Salvador en cuanto al cumplimiento de un SGSI

[4] *Organismo Salvadoreño de Normalización http://www.osn.gob.sv/index.php?option=com_k2&view=item&id=113:osn-realiza-evento-de-difusi%C3%B3n-de-normas-en-tecnolog%C3%ADa-de-la-informaci%C3%B3n&Itemid=79*

2.3.3. Métodos, técnicas e instrumentos

2.3.3.1. Metodología de la investigación

El trabajo de investigación realizado, comprende en la recopilación de datos primarios y secundarios, dentro de los cuales los datos primarios constituyen en toda la información proveniente del análisis de los resultados obtenidos en la encuesta y declaraciones emitidas por los propietarios o representantes de las empresas dentro del alcance de la investigación.

Los datos secundarios se han obtenido mediante una investigación documental, que incluye la revisión y consulta en páginas disponibles en internet, adaptación de normas en El Salvador, entre otros, que puedan ayudar a fortalecer la investigación sobre el tema en particular.

2.3.3.2. Determinación del objeto de estudio

El universo objeto del estudio está constituido por toda la empresa PYME salvadoreña, de 10 hasta 100 empleados, diferenciando entre pequeña empresa (10 - 50 empleados) y la mediana empresa (50 – 100 empleados).

El concepto de micro, pequeña y mediana empresa ha sido objeto de discusión por parte de diferentes instituciones, de entidades y de organizaciones gubernamentales y no gubernamentales; cada una de ellas utiliza diferentes parámetros para calificarlas en base a los objetivos propios que persiguen.

Para efectos de la definición y clasificación de las Pequeñas y Medianas empresas se utiliza los criterios y definiciones dados por el Ministerio de Economía de El Salvador.

Clasificación de las MIPYMES en El Salvador

Clasificación de empresas en El Salvador		
Clasificación	**Personal remunerado**	**Ventas brutas anuales / ingresos brutos anuales**
Microempresa	Hasta 10 empleados	Hasta USD$100,000.00
Pequeña empresa	Desde 10 hasta 50 empleados	Hasta USD $ 1,000,000.00
Mediana empresa	Desde 50 hasta 100 empleados	Hasta USD$ 7.0 millones
Gran empresa	Más de 100 empleados	Más de USD$ 7.0 millones

Fuente: Documento "El Salvador, generando riqueza desde la base: políticas y estrategias para la competitividad sostenible de las MIPYMES" del Ministerio de Economía de El Salvador

Tabla 4. Clasificación de las MIPYMES en El Salvador

Según datos de la Cámara de Comercio e Industria de El Salvador, en el país hay al menos 15,830 PYMES difundidos en todo el territorio nacional. El cuadro que se presenta a continuación refleja datos obtenidos de la Cámara Salvadoreña de Comercio e Industria hasta el año 2008.

Clasificación de las empresas en El Salvador y su porcentaje en el mercado

Clasificación	**Distribución**
Microempresa	90.52 %
Pequeña empresa	7.54 %
Mediana empresa	1.50 %
Sub total MIPYMES	99.56 %
Gran empresa	0.44 %
Total	100.00%

Tabla 5. Clasificación de las empresas en El Salvador y su porcentaje en el mercado

Fuente: sitio web de Cámara Salvadoreña de Comercio e Industria de El Salvador

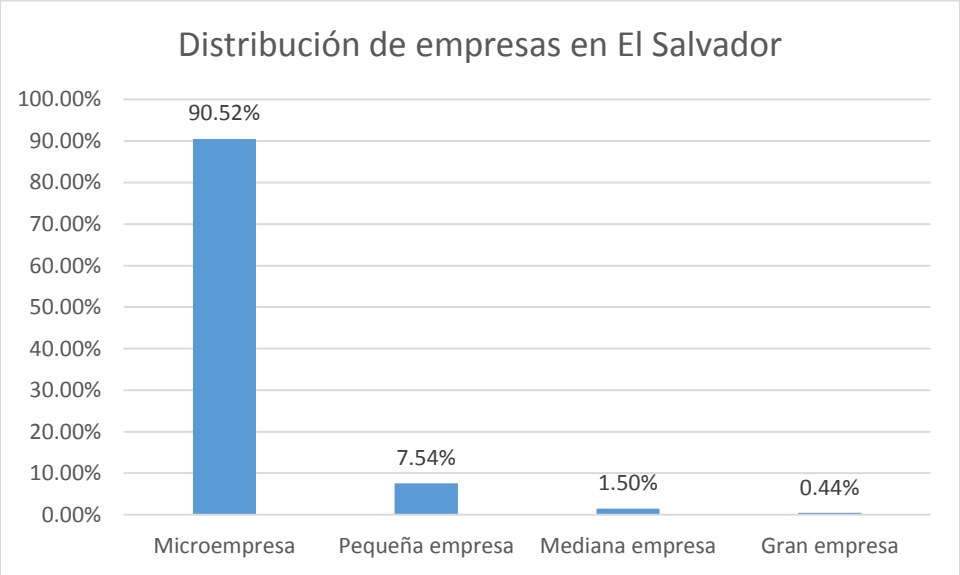

Figura 7. Distribución de empresas en El Salvador

2.3.3.3. Método

El método utilizado para la realización de la investigación ha sido basado en la técnica de la encuesta, se realizaron investigaciones sobre PYMES de diferentes rubros, cuyos propietarios, representantes y/o responsables de TI fueron el objeto de estudio.

2.3.3.4. Técnicas

Para desarrollar la investigación se utilizaron las técnicas siguientes: la encuesta, la entrevista dirigida y la observación directa; para la aplicación de estas técnicas se hizo uso del cuestionario y la observación directa.

2.3.3.5. Instrumento

El principal instrumento utilizado para realizar la investigación de campo es el cuestionario, el cual contiene preguntas que permiten determinar el cumplimiento de controles de seguridad para la implementación de un SGSI, el cuestionario fue diseñado para obtener información básica sobre temas de seguridad por parte de los propietarios, representantes y/o responsables de TI de cada una de las empresas investigadas.

La entrevista fue realizada a responsables de TI o a los propietarios de las empresas, quienes aportaron información detallada sobre el tema de investigación. Así mismo, para reforzar la información obtenida se realizó una observación directa durante las visitas a las empresas.

2.3.3.6. Unidades de análisis y sujetos de estudio

Las unidades de análisis están representadas por las PYMES dentro del alcance de la investigación desarrollada, las cuales corresponden a diferentes rubros, lo que permitió obtener una diversificación en la información para realizar puntos de análisis diferentes. Los sujetos de estudio fueron personas encuestadas de las empresas seleccionadas.

2.3.3.7. Población y muestra

Con base a la información obtenida de la Cámara Salvadoreña de Comercio e Industria el número de PYMES que se encuentran en el país es aproximadamente 15,380 que están distribuidas en los 261 municipios del país. El número total de PYMES representan el universo de la presente investigación.

2.3.3.8. Obtención de la muestra

Por tratarse de una población extensa y debido a la falta de cobertura, despliegue y por confidencialidad que poseen las mismas empresas, se obtuvieron únicamente información de diez empresas PYMES, dentro de las cuales se ha seleccionado empresas de los sectores de: Tecnología, Alimentos, Comercio, Jurídico, Logística, Educación y Servicios.

Para obtener la información de contactos de PYMES del país se realizó una solicitud a la Unidad de Acceso a la Información Pública y Transparencia de la Comisión Nacional de la Micro y Pequeña

Empresa de El Salvador (CONAMYPE), con respuesta a la solicitud se obtuvo la información de contacto de 10 empresas y se hizo de conocimiento que debido a motivos de confidencialidad en razón que la información requerida contiene datos personales, según lo establecido en el artículo 33 de la Ley de Acceso a la Información Pública de El Salvador, se proporcionó únicamente aquellos datos personales cuyos propietarios han autorizado expresa y libremente para ello.

2.3.3.9. Recolección de la información

La recolección de la información se realizó a través de:

a. Visita a CONAMYPE, por ser una institución que tiene como finalidad el desarrollo de la micro y pequeña empresa, nos abocamos a dicha institución para obtener la cantidad de PYMES registradas en El Salvador y debido a la cantidad proporcionada y por motivos de falta de cobertura, despliegue o confidencialidad de las mismas empresas, se han considerado únicamente cinco empresas, en las cuales encontramos disposición a proporcionar información, correspondientes a los sectores de logística, informática, contabilidad, producción y jurídico.
b. Se realizaron visitas a cada una de las empresas seleccionadas, encuestando a cada uno de los propietarios, representantes y/o responsables de TI de las mismas, durante dichas visitas se realizaron de forma simultánea entrevistas y observaciones directas.

2.3.3.10. Clasificación, registro y ordenamiento

Posterior a la recolección de los datos, la información se clasifico, ordeno y tabulo de forma manual, para luego ser procesada y presentada a través de tablas de distribución de frecuencia y sus correspondientes gráficos.

2.3.3.11. Análisis e interpretación de resultados

Se realizó un análisis crítico y exahustivo de los datos obtenidos en la investigación para definir el criterio de aplicabilidad y/o cumplimiento de los controles del apartado 5 “Guía de implementación, métricas y mediciones” de la norma NTS ISO/IEC 27001:2013, con la finalidad de adecuar los requisitos de dicha norma para la implementación, cumplimiento y medición de un SGSI a la medida de la PYME Salvadoreña.

Encuesta para la evaluación de la gestión de la seguridad de la información en la PYME Salvadoreña. Dirigida a representantes y/o encargados de TI.

Parte I: Datos generales

Pregunta No. 1

Aproximadamente, ¿de cuántas computadoras dispone su empresa?

Objetivo 1: Determinar la cantidad de computadoras que dispone la empresa

Alternativa	Frecuencia	Porcentaje
De 1 a 5	**1**	10%
De 5 a 10	**4**	40%
De 10 a 20	**5**	50%
Ninguna	**0**	0%
Total	**10**	**100%**

Tabla 6. Pregunta No. 1

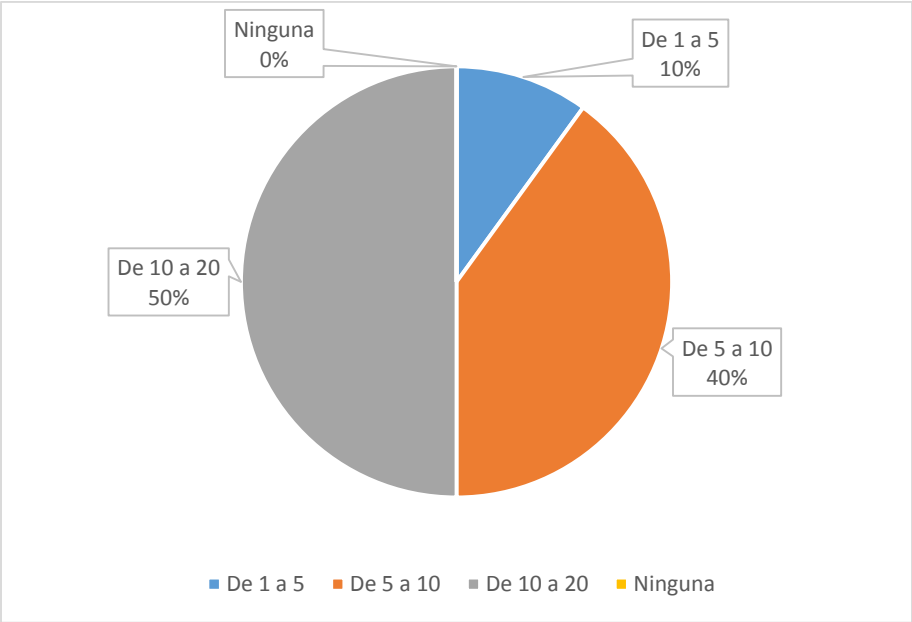

Gráfico 1. Pregunta No. 1

Análisis: Con base a las respuestas obtenidas, se determinó que un 50% de la muestra cuenta con un número de computadoras que va de 10 a 20 equipos. Lo que demuestra que al menos el 50% de las PYMES encuestadas poseen infraestructura tecnológica compleja la cual debe ser debidamente gestionada.

Pregunta No. 2

Aproximadamente, ¿de cuántos empleados dispone su empresa?

Objetivo 2: Determinar el ámbito y tamaño de la empresa

Alternativa	Frecuencia	Porcentaje
De 2 a 10	**1**	10%
De 11 a 25	**1**	10%
De 26 a 50	**6**	60%

A partir de 50	**2**	20%
Total	**10**	**100%**

Tabla 7. Pregunta No. 2

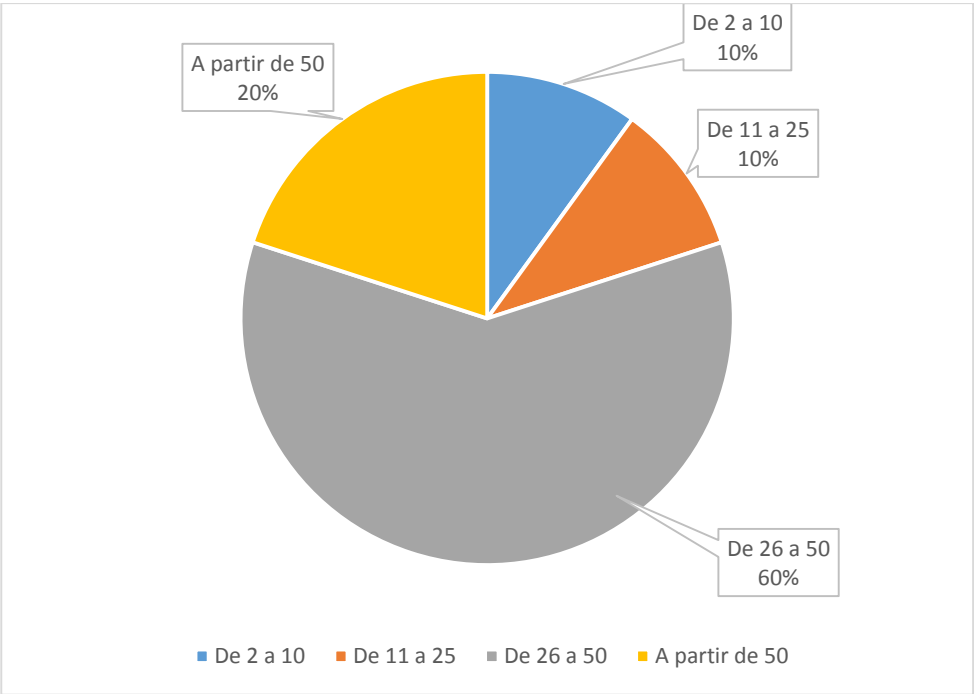

Gráfico 2. Pregunta No. 2

Análisis: De acuerdo a los encuestados el 90% de éstas empresas son pequeñas y medianas y solo un 10% son micro empresas. Lo que demuestra que los resultados obtenidos en la encuesta corresponden en su mayoría al sector objetivo del presente trabajo.

Pregunta No. 3

En su empresa, la seguridad es:

Objetivo 3: Conocer el grado de interés de las empresas en cuanto a la seguridad de la información

Alternativa	Frecuencia	Porcentaje
Muy importante	**4**	40%
Importante	**5**	50%
Nada importante	**1**	10%
Total	10	100%

Tabla 8. Pregunta No. 3

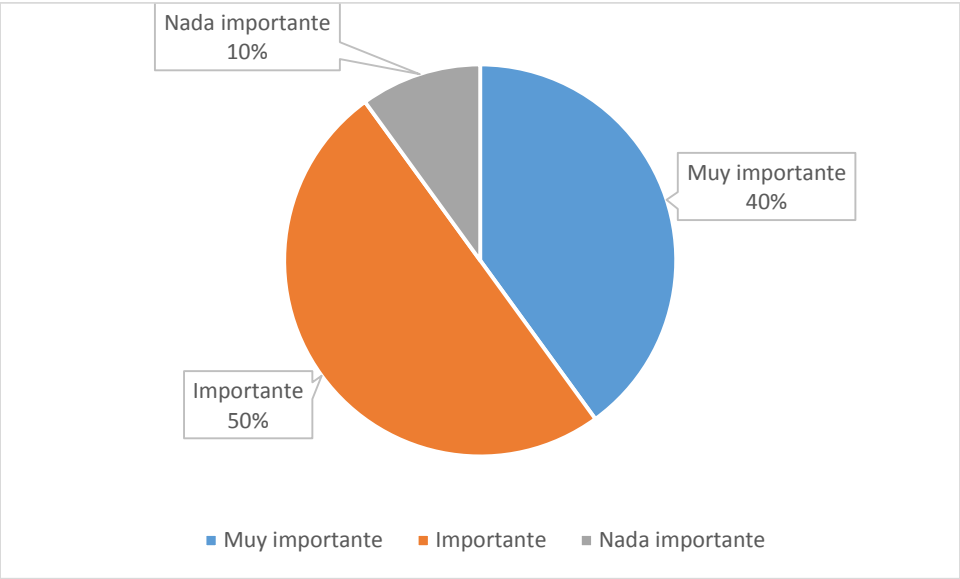

Gráfico 3. Pregunta No. 8

Análisis: Con base a los resultados obtenidos es posible determinar que un 90% de las empresas encuestadas considera la seguridad de la información como un tema importante o muy importante, mientras que un 10% no lo considera un tema prioritario, lo cual nos indica que la mayor parte de las empresas están conscientes de la importancia de la seguridad de la información.

Pregunta No. 4

¿Utiliza en su empresa, algún sistema de seguridad?

Objetivo 4: Identificar el estado actual del uso de sistemas de seguridad en la PYME salvadoreña

Alternativa	Frecuencia	Porcentaje
Si	**8**	80%
No	**2**	20%
No se	**0**	0%
Total	**10**	**100%**

Tabla 9. Pregunta No. 4

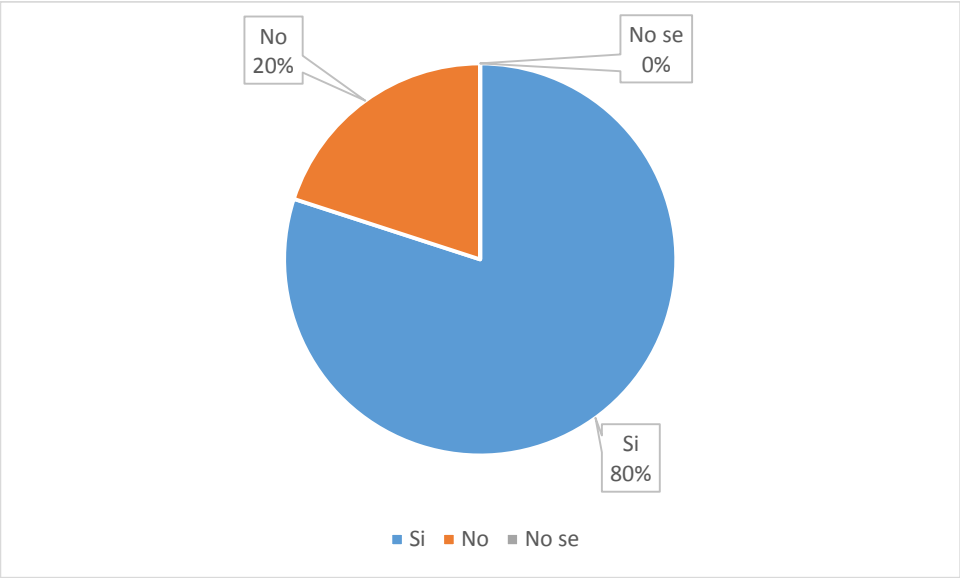

Gráfico 4. Pregunta No. 4

Análisis: En cuanto al uso de sistemas de seguridad en las empresas encuestadas el 80% por ciento mencionó que poseen al menos un sistema de seguridad instalado en sus equipos de cómputo, lo que permite determinar que existe cierto nivel de esfuerzos por parte de éstas empresas para garantizar la seguridad de la información.

Pregunta No. 5

¿Considera necesario invertir en un sistema de seguridad de la información?

Objetivo 5: Determinar la posición de la empresa con respecto a la inversión que se debe realizar para la adquisición y uso de sistemas de seguridad de la información

Alternativa	Frecuencia	Porcentaje
No es necesario / no es importante	**0**	0%
Los sistemas de seguridad consumen muchos recursos	**1**	10%
Es caro	**0**	0%
No tiene / no usan ordenador	**0**	0%
Si / lo están estudiando	**9**	90%
Total	**10**	**100%**

Tabla 10. Pregunta No. 5

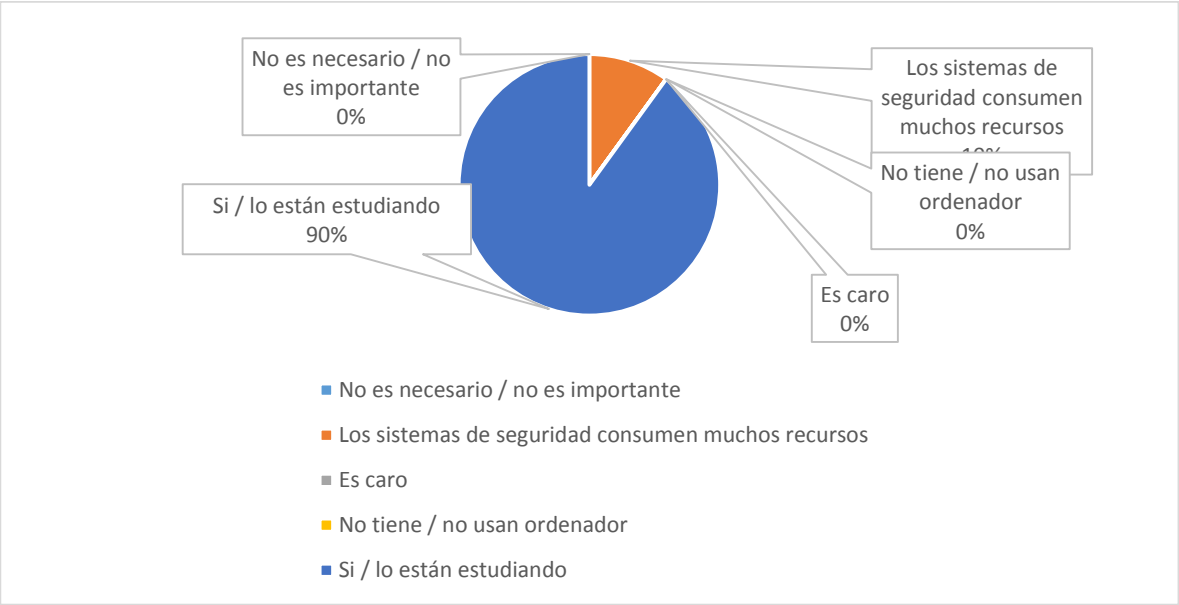

Gráfico 5. Pregunta No. 5

Análisis: Los resultados muestran que el mayor porcentaje de las empresas encuestadas considera necesario invertir en un sistema de seguridad de la información. Esta situación podría ser resultado del nivel de concientización de las empresas con respecto a temas de seguridad de la información.

Pregunta No. 6

¿Qué presupuesto destina anualmente a las soluciones de seguridad de la información?

Objetivo 6: Detectar el monto anual que la empresa destina para adquirir y/o utilizar algún tipo de solución de seguridad de la información

Alternativa	Frecuencia	Porcentaje
Menos de $100	**2**	20%
Entre $100 y $300	**7**	70%
Entre $300 y $500	**1**	10%
Entre $500 y $1000	**0**	0%
Más de $1000	**0**	0%
Total	10	100%

Tabla 11. Pregunta No. 6

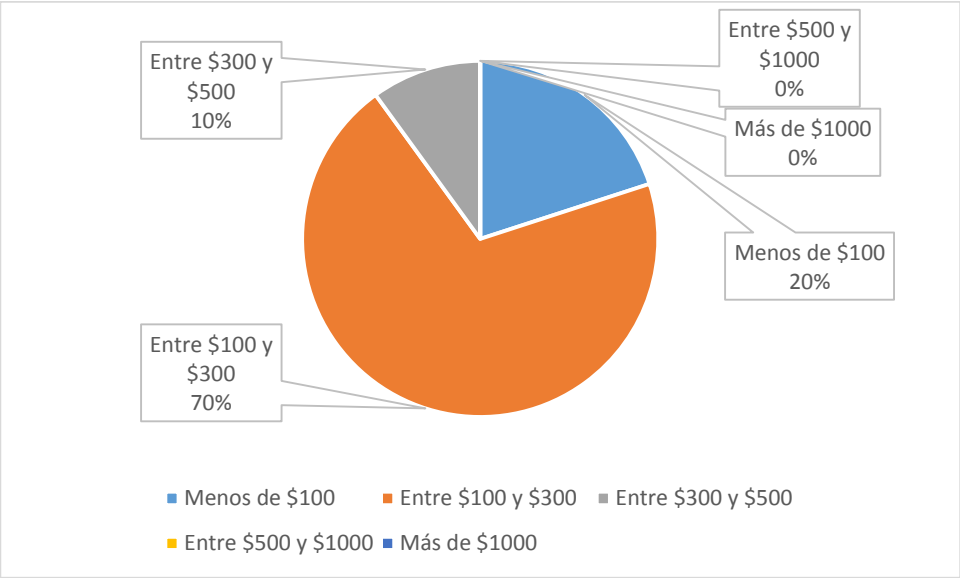

Gráfico 6. Pregunta No. 6

Análisis: Entre el 70% y 80% de las empresas encuestadas realiza una inversión en seguridad de la información valorada entre 100 y 500 dólares, demostrando que existe un compromiso de la dirección de la empresa en obtener una solución de seguridad de la información.

Parte II: Política de Seguridad de la información

Gestión de la dirección para la seguridad de la información

Objetivo: Proporcionar directrices y apoyo para la seguridad de la información en concordancia con los requerimientos del negocio, leyes y regulaciones pertinentes.

Pregunta No. 7

¿Tiene su empresa una política de seguridad de la información aprobada, publicada y comunicada a los empleados?

Objetivo 7: Determinar si la empresa cuenta con un documento de política de seguridad de la información el cual se encuentre definido y aprobado por la dirección

Alternativa	Frecuencia	Porcentaje
Si, ha sido aprobada	**1**	10%
Si, ha sido aprobada y publicada	**1**	10%
Si, ha sido aprobada, publicada y comunicada	**1**	10%
No	**7**	70%
Total	10	100%

Tabla 12. Pregunta No. 7

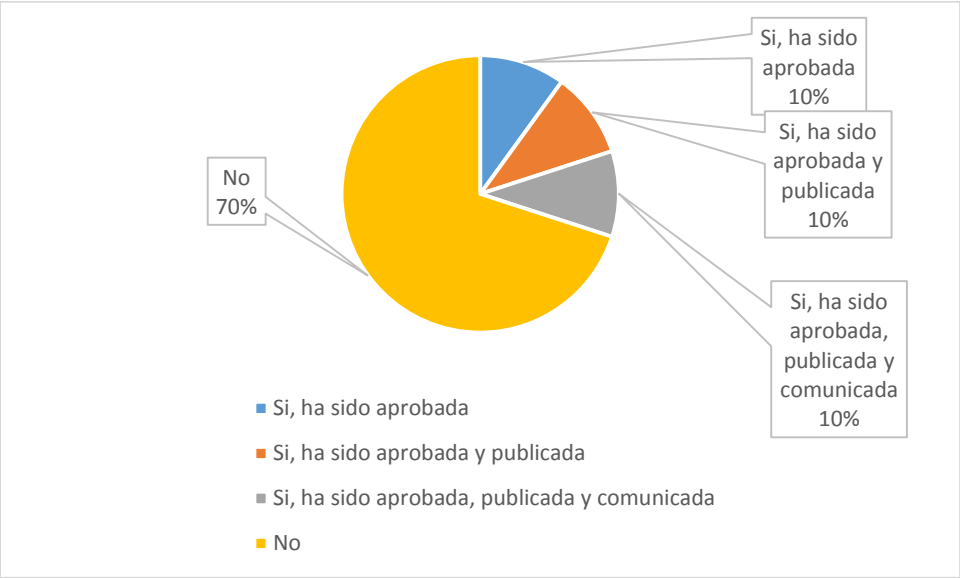

Gráfico 7. Pregunta No. 7

Análisis 7: Si bien es cierto el 30% de las PYMES encuestadas poseen una política de seguridad, existe un alto porcentaje de ellas que no cuenta con éste documento, por lo que es posible determinar que el 70% de las empresas carecen de una adecuada gestión de la seguridad de la información.

Recomendación:

La dirección debe definir una política de seguridad de la información de acuerdo a las características del negocio, su organización, sus activos y a la tecnología que ésta posee.

Pregunta No. 8

¿Realiza revisiones periódicas a la política de seguridad de la información?

Objetivo 8: Determinar si existe un proceso de mejora continua de la política de seguridad de la información.

Alternativa	Frecuencia	Porcentaje
Si	**0**	0%
No	**10**	100%
Total	10	100%

Tabla 13. Pregunta No. 8

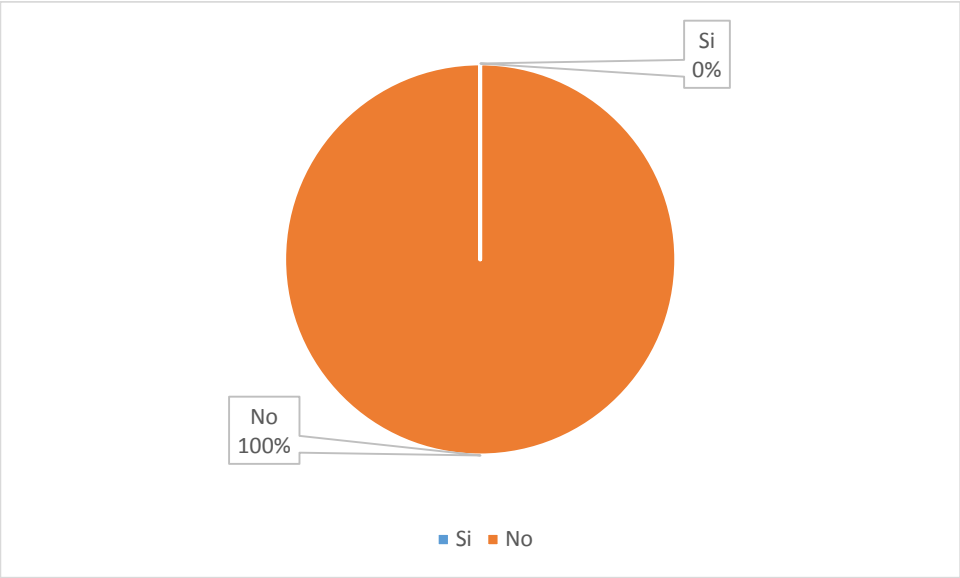

Gráfico 8. Pregunta No. 8

Análisis 8: Aunque en la pregunta 7 se identificó que el 30% de las empresas encuestadas cuentan con una política de seguridad documentada, autorizada y publicada, éstas no realizan revisiones periódicas lo que demuestra que no existe un proceso de mejora continua sistematizado.

Recomendación 8:

La dirección debe evidenciar el compromiso con la mejora continua a través de revisiones periódicas de la política de seguridad de la información para asegurar que se mantenga su continuidad y efectividad.

Parte III: Aspectos organizativos de la seguridad de la información

Organización interna

Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización

Pregunta No. 9

¿Cuenta su empresa con una o más personas dedicadas a la seguridad informática?

Objetivo 9: Identificar si existen responsabilidades definidas y asignadas en la empresa en cuanto a la seguridad de la información

Alternativa	Frecuencia	Porcentaje
Si	**3**	30%
No	**7**	70%
Total	10	100%

Tabla 14. Pregunta No. 9

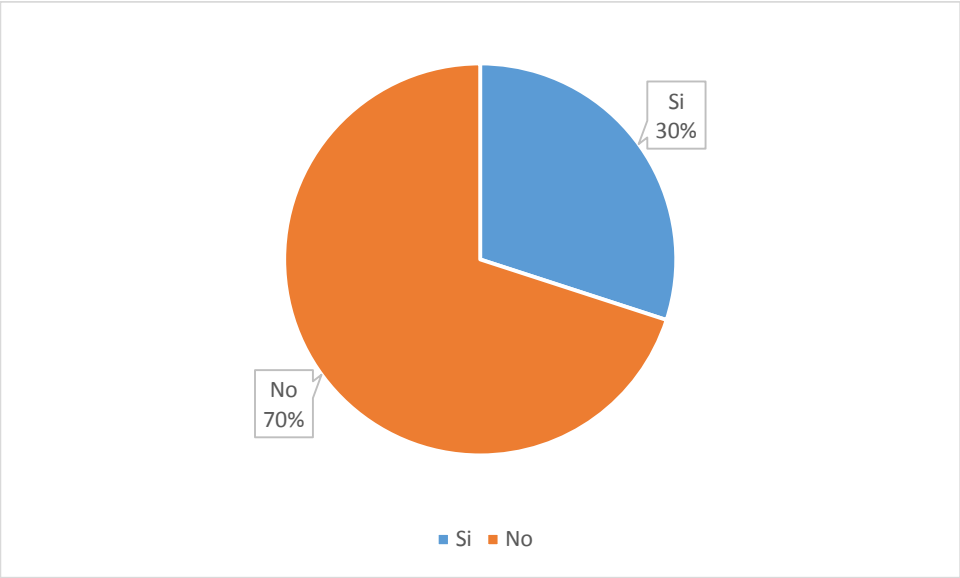

Gráfico 9. Pregunta No. 9

Análisis 9: Los resultados indican que el mayor parte de las empresas encuestadas no existen responsabilidades definidas y asignadas en cuanto a la seguridad de la información.

Recomendación 9:

Debe existir una segregación de funciones orientado a los temas de seguridad de la información, debidamente documento en el manual de puestos.

Pregunta No. 10

¿Cuándo necesita información o asesoramiento sobre temas de seguridad informática a quién le pide consejo?

Objetivo 2: Detectar si existe un flujo adecuado de asesoramiento de temas de seguridad a través de grupos de interés y/o asociaciones profesionales especializadas en seguridad

Alternativas	Frecuencia	Porcentaje
A nadie	**2**	20%
Soporte técnico/técnico especializado	**2**	20%
Vendedor / Comercial	**1**	10%
Internet	**4**	40%
Fabricante/web del fabricante	**0**	0%
Otro	**1**	10%
Total	**10**	100%

Tabla 15. Pregunta No. 10

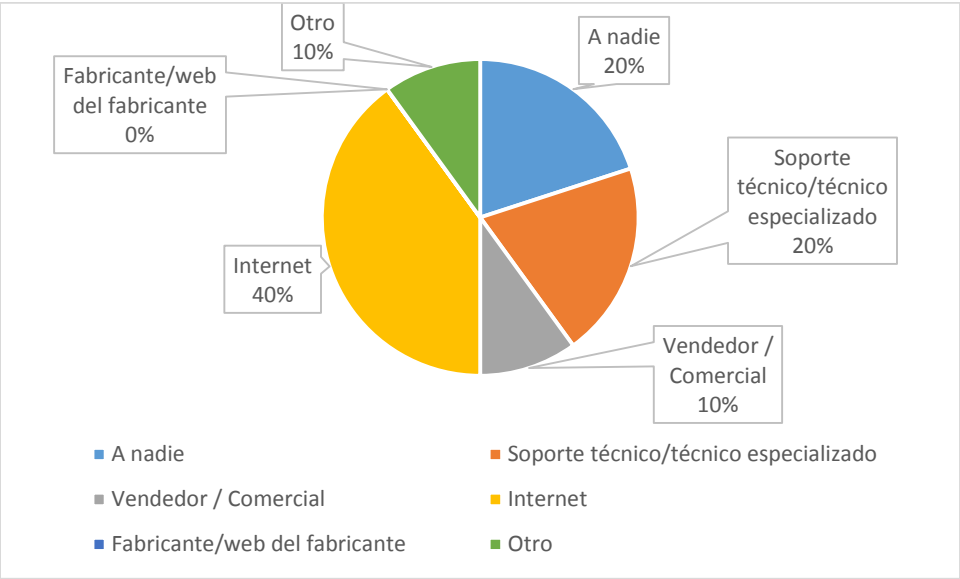

Gráfico 10. Pregunta No. 10

Análisis 10: Los datos presentan que únicamente un 20% de las empresas encuestadas busca soporte adecuado y asesoramiento de temas de seguridad con personal especializado.

Recomendación 10: Se debería mantener el contacto con grupos o foros de seguridad especializados y asociaciones profesionales.

Pregunta No. 11

¿La seguridad de la información es un componente que se toma en cuenta durante la formulación y ejecución de los proyectos?

Objetivo 11: Conocer el trato de la seguridad de la información en la gestión de cualquier proyecto de la empresa

Alternativa	Frecuencia	Porcentaje
Si	**2**	20%
No	**8**	80%
Total	**10**	100%

Tabla 16. Pregunta No. 11

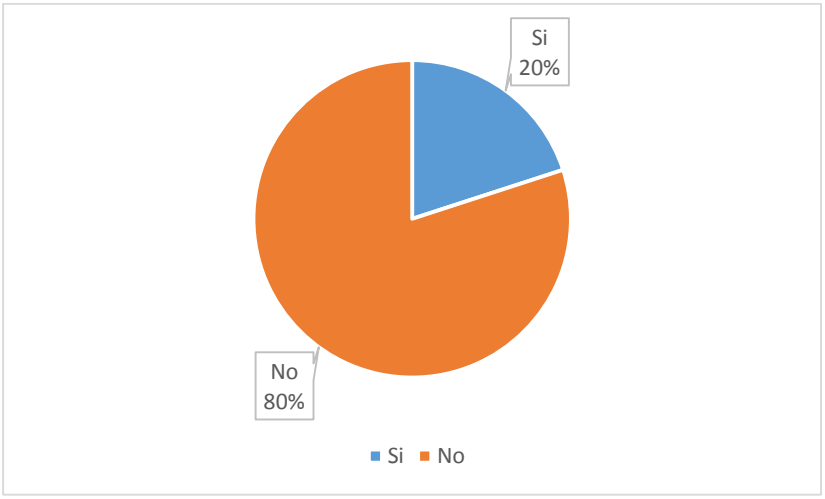

Gráfico 11. Pregunta No. 11

Análisis 11: Los datos reflejan que solamente el 20% de las empresas encuestadas toman en cuenta la seguridad de la información como un componente para el desarrollo de proyectos.

Recomendación 11: Se debe contemplar la seguridad de la información en la gestión de los proyectos de la organización, independientemente del tipo de proyecto.

Dispositivos móviles y trabajo remoto

Objetivo: Asegurar la seguridad del trabajo remoto y el uso de dispositivos móviles

Pregunta No. 12

¿Dispone de alguna política para el uso seguro de dispositivos móviles (smartphone, PDA, tablets, etc)?

Objetivo 12: Determinar si la empresa cuenta con un documento de política y medidas de soporte de seguridad para la gestión de riesgos en el uso de dispositivos móviles

Alternativa	Frecuencia	Porcentaje
Si	**0**	0%
No	**10**	100%
No se	**0**	0%

Tabla 17. Pregunta No. 12

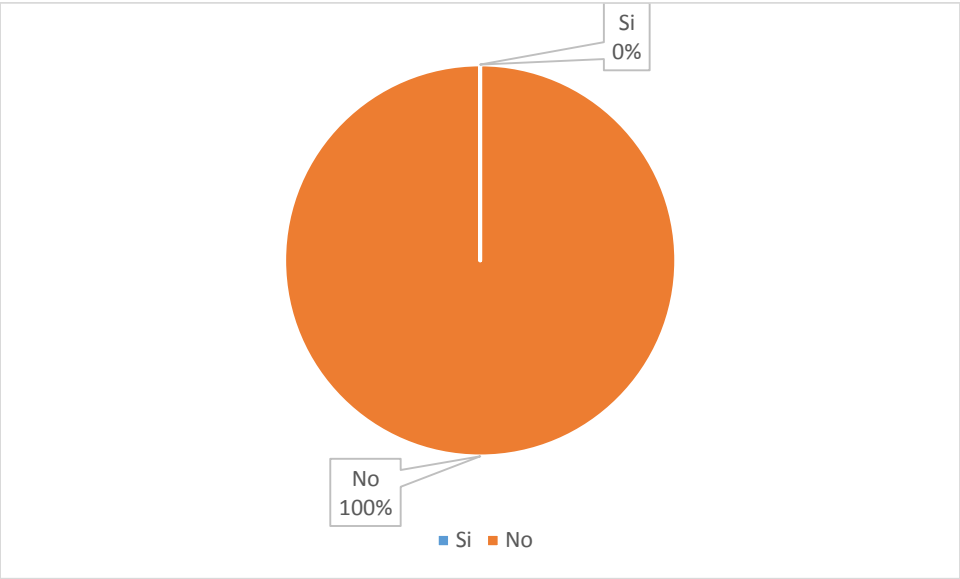

Gráfico 12. Pregunta No. 12

Análisis 12: Ninguna de las empresas encuestadas posee un documento donde se establecen la política y medidas de seguridad para los dispositivos móviles.

Recomendación 12: Se debería establecer una política de seguridad para dispositivos móviles y se debería adoptar las medidas de seguridad adecuadas para la protección contra el riesgo por el uso de tecnología móvil.

Pregunta No. 13

¿Existe alguna política y medidas de seguridad implementadas para proteger la información accedida, procesada o almacenada en sitios de trabajo remoto?

Objetivo 13: Determinar si la empresa cuenta con un documento de política y medidas de soporte de seguridad para la protección de la información accedida, procesada o almacenada en sitios de trabajo remoto

Alternativa	Frecuencia	Porcentaje
Si	**0**	0%
No	**10**	100%
No se	**0**	0%
Total	**10**	100%

Tabla 18. Pregunta No. 13

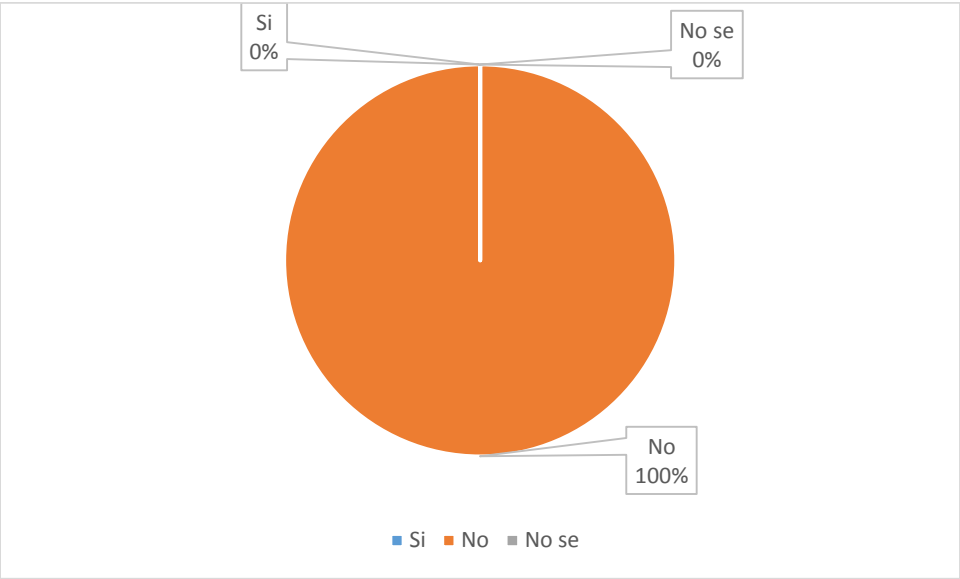

Gráfico 13. Pregunta No. 13

Análisis 13: Es claro que el 100% de las empresas no adoptan medidas de soporte a través de una política de seguridad para la protección de la información accedida o procesada a través de sitios de trabajo remoto.

Recomendación 13: Se debería establecer una política para la protección de la información que es accedida y procesada a través de sitios remotos.

Parte IV: Seguridad de los recursos humanos

Antes del empleo

Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y sean idóneos para los roles para los cuales se les considera

Pregunta No. 14

¿Se recopila y verifica la información necesaria (referencias, currículum, etc) y se comprueba la adecuación de los candidatos para el puesto para el que son requeridos?

Objetivo 14: Identificar la existencia de controles de verificación de antecedentes de los candidatos para el empleo

Alternativa	Frecuencia	Porcentaje
Si	**10**	100%
No	**0**	0%
Total	10	100%

Tabla 19. Pregunta No. 14

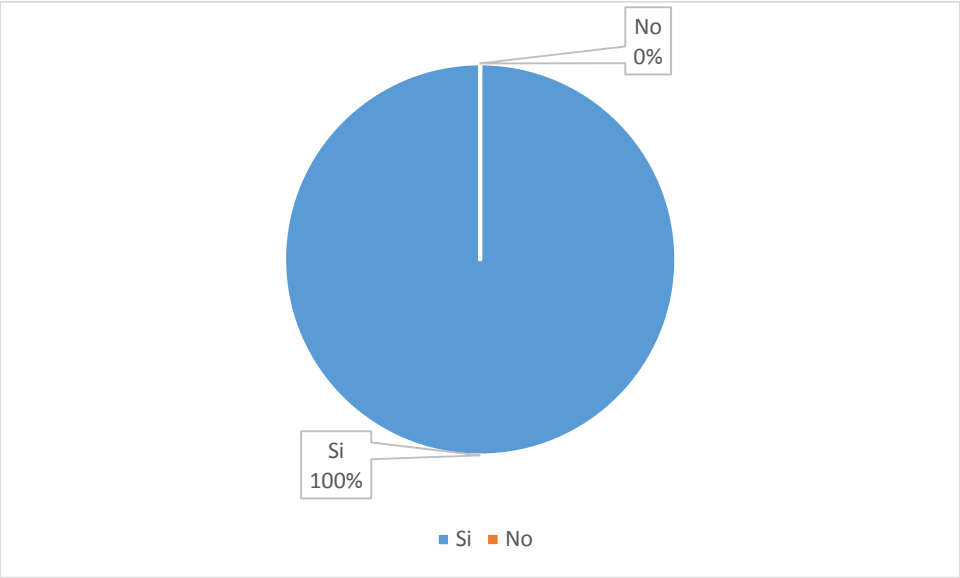

Gráfico 14. Pregunta No. 14

Análisis 14: Las empresas encuestadas reflejan un 100% en la implementación de controles para verificación de antecedentes de los candidatos para el empleo.

Recomendación 14: Las empresas deben poseer controles de recopilación y verificación de información necesaria que compruebe la adecuación de los candidatos para el perfil que lo ha requerido.

Pregunta No. 15

¿Los contratos, contienen las clausulas necesarias para garantizar el cumplimiento de requisitos de seguridad?

Objetivo 15: Conocer si los acuerdos contractuales de la empresa contienen todas las clausulas necesarias para establecer las responsabilidades de los empleados y garantizar requisitos de la seguridad de la información.

Alternativa	Frecuencia	Porcentaje
Si	**5**	50%
No	**5**	50%
Total	**10**	**100%**

Tabla 20. Pregunta No. 15

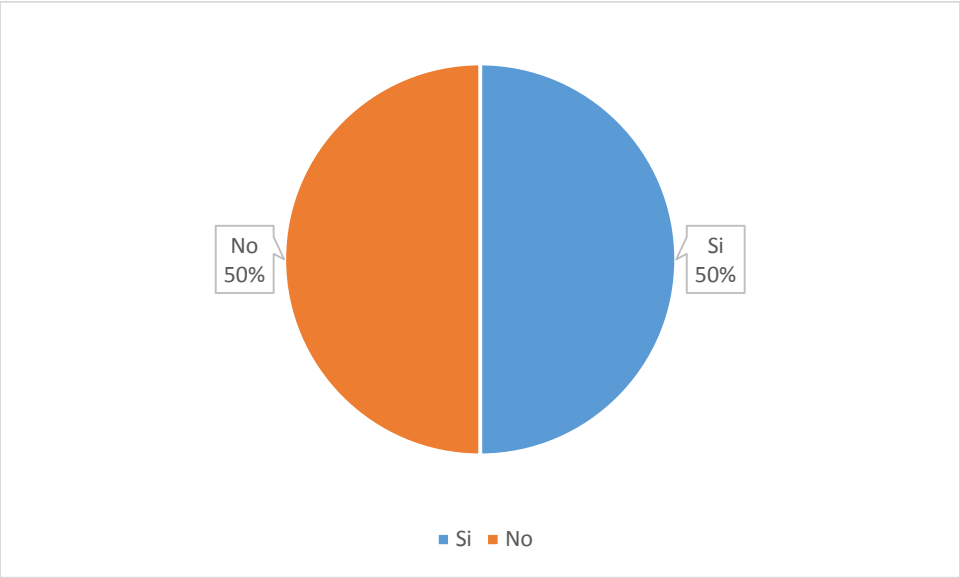

Gráfico 15. Pregunta No. 15

Análisis 15: Se puede observar que existe igual porcentaje entre las empresas que dentro de los contratos de los empleados incluyen o no clausulas necesarias para garantizar el cumplimiento de los requisitos de seguridad.

Recomendación 15: La empresa debe incluir en los contratos de empleo términos y condiciones a través de las cuales se establezca los compromisos de los empleados para con la seguridad de la información.

Durante el empleo

Objetivo: Asegurar que todos los empleados y contratistas estén conscientes de cumplir con sus responsabilidades de la seguridad de la información.

Pregunta No. 16

¿Es requerido el cumplimiento de las políticas y procedimiento de seguridad de la empresa a los empleados y prestadores de servicios?

Objetivo 16: Detectar si existe un requerimiento a los empleados y contratistas para el cumplimiento de la seguridad de la información en base a políticas y procedimientos establecidos por la organización

Alternativa	Frecuencia	Porcentaje
Si	**4**	40%
No	**6**	60%
Total	**10**	**100%**

Tabla 21. Pregunta No. 16

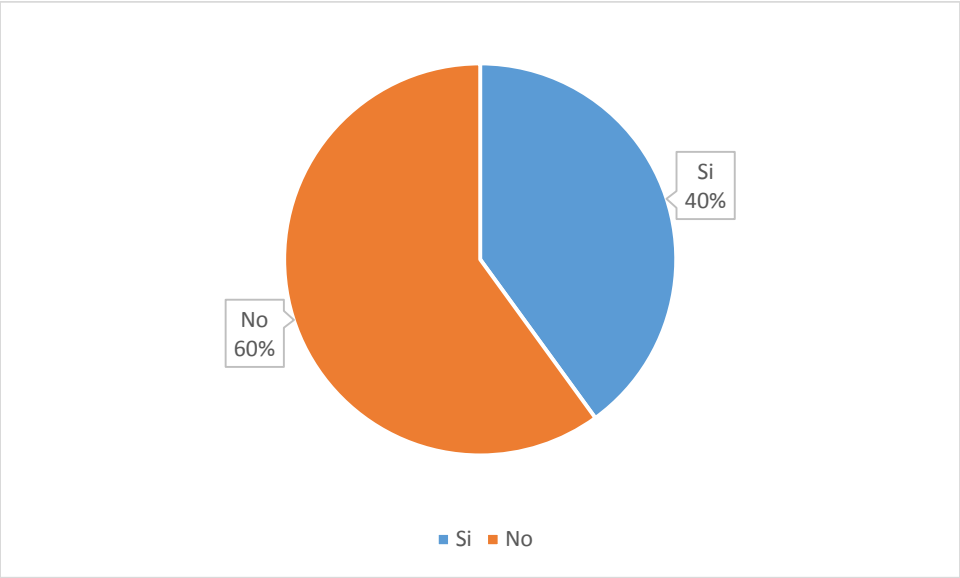

Gráfico 16. Pregunta No. 16

Análisis 16: El 40% de las empresas encuestadas cuenta con un documento donde se requiere a los empleados y contratistas el cumplimiento de medidas para la seguridad de la información, mientras que el 60% no poseen ningún soporte donde se requiera el cumplimiento de éste tipo de medidas.

Recomendación 16: La Dirección debe asegurar que los empleados y prestadores de servicio dan cumplimiento a las políticas y procedimientos de seguridad de la empresa.

Pregunta No. 17

¿Recibe usted o los empleados de su empresa formación relacionada sobre la seguridad informática, y las amenazas actuales que pueden afectarle?

Objetivo 17: Determinar si se imparte una adecuada concientización y capacitación de las políticas y procedimientos de la empresa a los empleados y contratistas y a su vez, conocer si existe algún tipo de inversión para la realización de la misma.

Alternativa	Frecuencia	Porcentaje
Si, gratuita	**0**	0%
Si, de pago	**1**	10%
No, ninguna	**9**	90%
Total	**10**	100%

Tabla 22. Pregunta No. 17

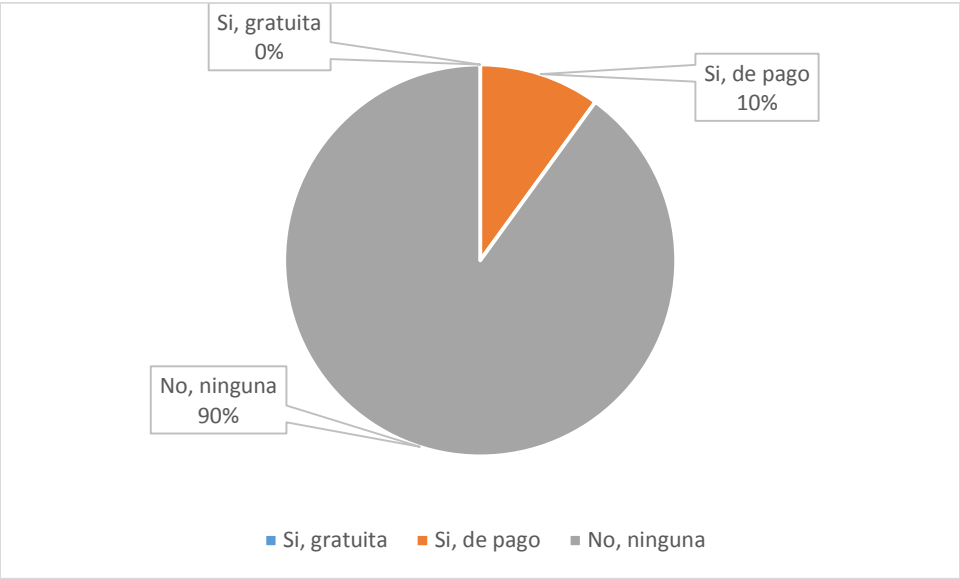

Gráfico 17. Pregunta No. 17

Análisis 17: En cuanto a la formación y concientización que reciben los empleados en temas de seguridad de la información, los datos nos indican que existe un alto porcentaje de las empresas encuestadas que no brinda a sus empleados una adecuada inducción y capacitación en políticas y procedimientos relevantes a la seguridad de la información.

Recomendaciones 17: La organización debe establecer un procedimiento de formación y concientización a los empleados sobre la relevancia de seguridad de la información.

Pregunta No. 18

¿Existe un proceso disciplinario para empleados y prestadores de servicios que se aplica cuando incumplen las políticas y procedimientos?

Objetivo 18 Determinar la existencia de un proceso disciplinario formal el cual debe ser aplicado a cualquier empleado o contratista que cometa cualquier tipo de violación en la seguridad de la información.

Alternativa	Frecuencia	Porcentaje
Si	**5**	50%
No	**5**	50%
Total	10	100%

Tabla 23. Pregunta No. 18

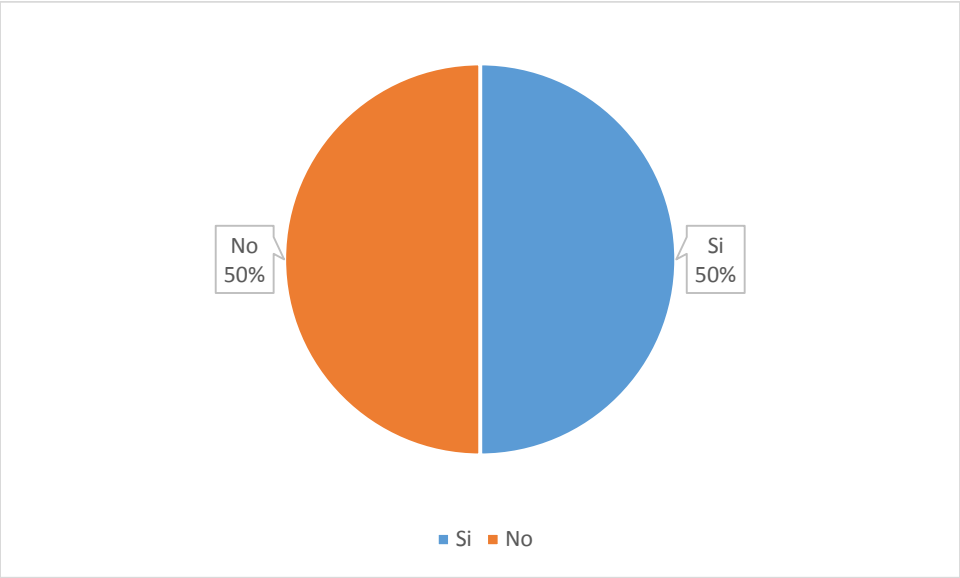

Gráfico 18. Pregunta No. 18

Análisis 18: Los resultados ponen evidencia que al menos la mitad de las empresas encuestadas carecen de procesos disciplinarios formales para garantizar que tanto los empleados como los contratistas dan cumplimiento a la política, procedimientos y medidas de seguridad de la información.

Recomendaciones 18: La organización debe asegurar que existe un proceso disciplinario que tome acción en contra de empleados o terceros que cometan una violación a las políticas de seguridad de la empresa.

Terminación y cambio de empleo

Objetivo: Proteger los intereses de la organización como parte de un proceso de terminación o cambio de empleo.

Pregunta No. 19

¿Se establecen responsabilidades de terminación o cambio de contrato para empleados o proveedores?

Objetivo 19: Determinar la definición y comunicación de responsabilidades y funciones de la seguridad de la información a los empleados y contratistas, las cuales deben permanecer validas después de una terminación o cambio de empleo

Alternativa	Frecuencia	Porcentaje
Si	**1**	10%
No	**9**	90%
Total	10	100%

Tabla 24. Pregunta No. 19

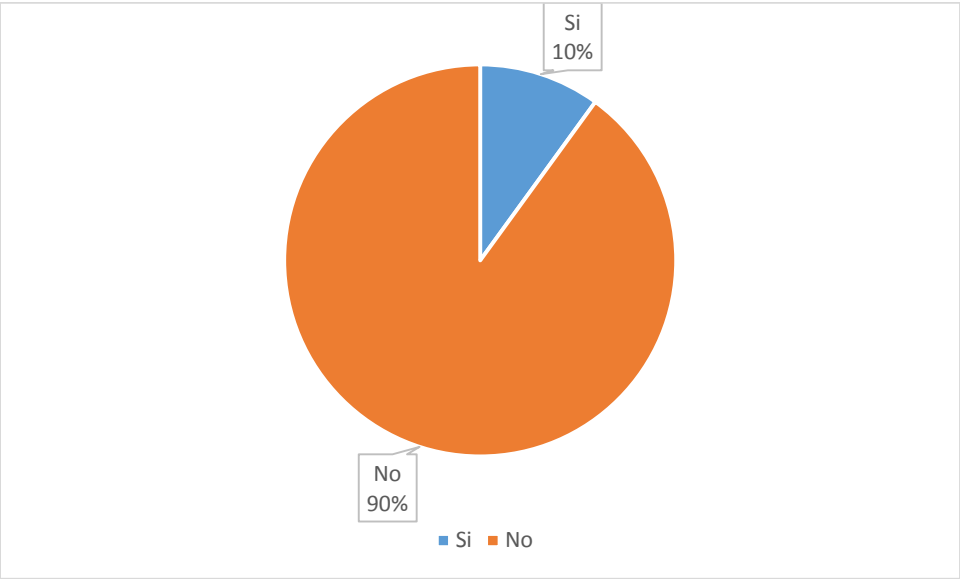

Gráfico 19. Pregunta No. 19

Análisis 19: De acuerdo a los resultados obtenidos un 90% de las empresas encuestadas no establecen medidas de terminación o cambio de contrato para empleados o proveedores, situación que podría generar una afectación en el manejo adecuado de los activos de información.

Recomendación 19: Se debería establecer las responsabilidades para asegurar que el abandono de la organización por parte de los empleados o contratistas se controla.

Parte V: Gestión de activos

Responsabilidad sobre los activos

Objetivo: Identificar los activos organizacionales y definir las apropiadas responsabilidades de protección.

Pregunta No. 20

¿Cuenta la empresa con un inventario de activos actualizado?

Objetivo 20: Identificar la existencia de un inventario de activos en la empresa

Alternativa	Frecuencia	Porcentaje
Si	**7**	70%
No	**3**	30%
Total	10	100%

Tabla 25. Pregunta No. 20

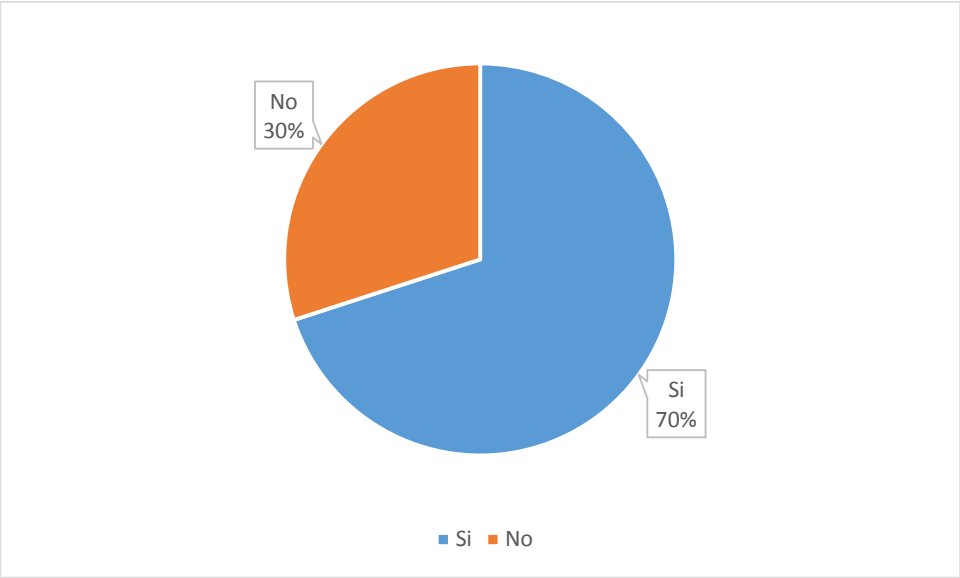

Gráfico 20. Pregunta No. 20

Análisis 20: El 70% de las empresas encuestadas tienen identificados claramente los activos a través de un inventario registrado, mientras que el 30% restante no mantiene un inventario de sus activos.

Recomendación 20: Los activos deben estar identificados, registrados y asignados.

Pregunta No. 21

¿Los activos se encuentran asignados?

Objetivo 21: Determinar si se realiza la asignación de activos dentro de la empresa

Alternativa	Frecuencia	Porcentaje
Si	**8**	80%
No	**2**	20%
Total	10	100%

Tabla 26. Pregunta No. 21

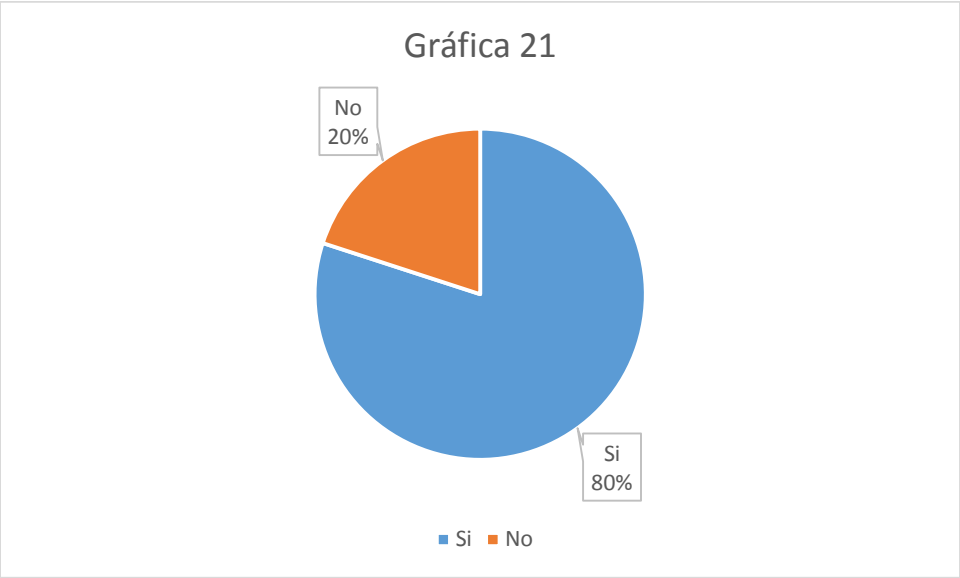

Gráfico 21. Pregunta No. 21

Análisis 21: El 80% de las empresas encuestadas cuentan con registros de asignación de activos al personal, si comparamos con el dato obtenido en la pregunta 20 es posible afirmar que del 80% de las empresas que cuenta con la asignación de activos el 70% cuenta con un inventario formal de éstos.

Recomendación 21: Todos los activos deben estar debidamente asignados.

Pregunta No. 22

¿Existe algún documento que establezca el uso aceptable de los activos?

Objetivo 22: Identificar la existencia de un documento donde se definan las reglas para el uso aceptable de la información y los activos asociados

Alternativa	Frecuencia	Porcentaje
Si	**4**	40%
No	**6**	60%
Total	10	100%

Tabla 27. Pregunta No. 22

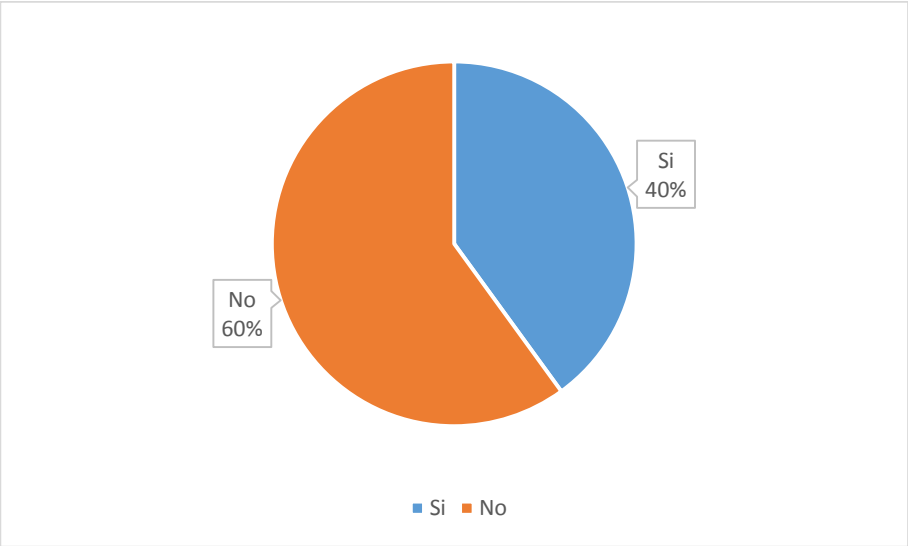

Gráfico 22. Pregunta No. 22

Análisis 22: Los resultados obtenidos reflejan que el 40% de las empresas cuenta con un documento donde se define el uso aceptable de la información y los activos asociados.

Recomendación 22: Se debe identificar y documentar las reglas para el uso adecuado de la información y los activos asociados.

Pregunta No. 23

¿Al finalizar la relación contractual con los empleados o usuarios externos, existe algún procedimiento para la devolución de activos?

Objetivo 23: Determinar la existencia de procedimientos al momento de terminación del contrato de los empleados y usuarios externos, donde especifique que deben devolver todos los activos de la organización que se encuentren en su posesión

Alternativa	Frecuencia	Porcentaje
Si	**5**	50%
No	**5**	50%
Total	10	100%

Tabla 28. Pregunta No. 23

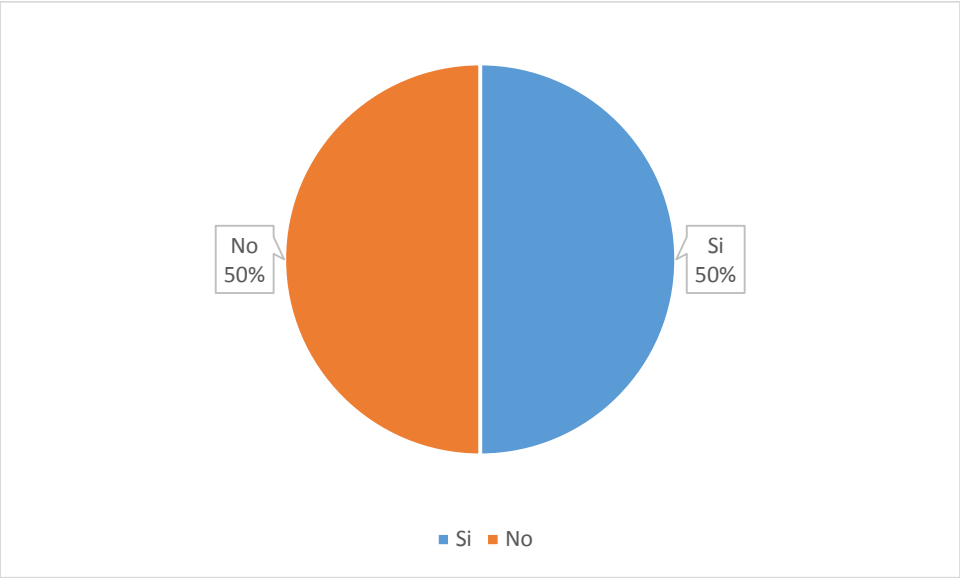

Gráfico 23. Pregunta No. 23

Análisis 23: Los resultados obtenidos indican una paridad entre las empresas que tienen definido un procedimiento para la devolución de activos al momento de la terminación del contrato de usuarios internos o externos.

Recomendación 23: Todos los empleados y usuarios de terceras partes deben devolver todos los activos de la organización que estén bajo su responsabilidad una vez finalizado el contrato de empleo o de prestación de servicios.

Clasificación de la información

Objetivo: Asegurar que la información reciba un nivel apropiado de protección en concordancia con su importancia para la organización.

Pregunta No. 24

¿La información se encuentra clasificada y etiquetada en términos de su valor, requerimientos legales, sensibilidad y criticidad?

Objetivo 24: Determinar si dentro de la empresa existe una clasificación de la información según su tipo

Alternativa	Frecuencia	Porcentaje
Si	**0**	0%
No	**10**	100%
Total	10	100%

Tabla 29. Pregunta No. 24

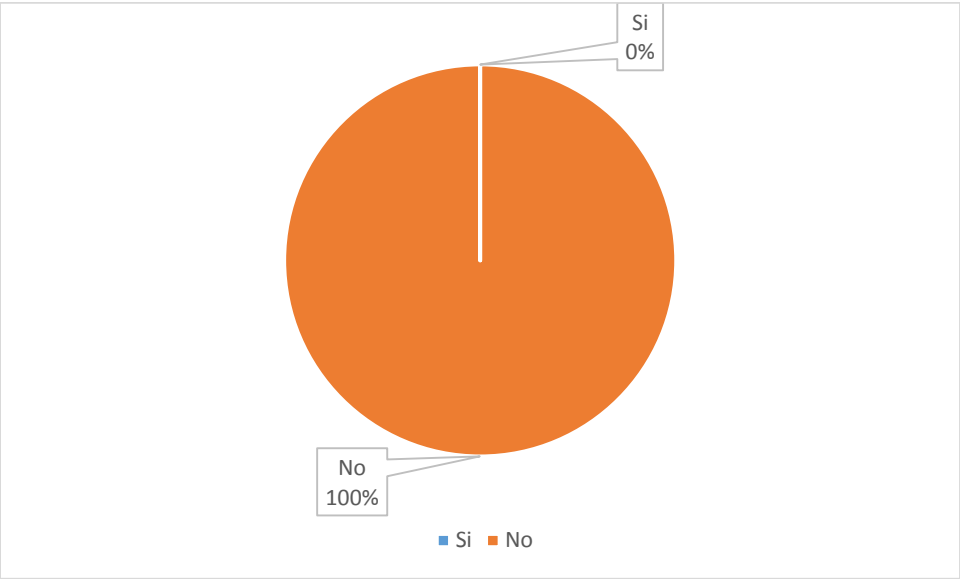

Gráfico 24. Pregunta No. 24

Análisis 24: Es claro que en el 100% de las empresas encuestas no existe una clasificación de la información en términos de su valor. Esto pone en evidencia el grado vulnerabilidad que existe con respecto a la confidencialidad, integridad y disponibilidad de la información.

Recomendación 24: La organización debe distinguir los requisitos mínimos de seguridad para una adecuada clasificación de la información tomando como referencia los parámetros de grado de confidencialidad, requisitos de disponibilidad e integridad.

Pregunta No. 25

¿Se cuenta con procedimientos definidos para el manejo de información según su clasificación?

Objetivo 25: Identificar la existencia de procedimientos para el manejo de la información según su clasificación

Alternativa	Frecuencia	Porcentaje
Si	**0**	0%
No	**10**	100%
Total	10	100%

Tabla 30. Pregunta No. 25

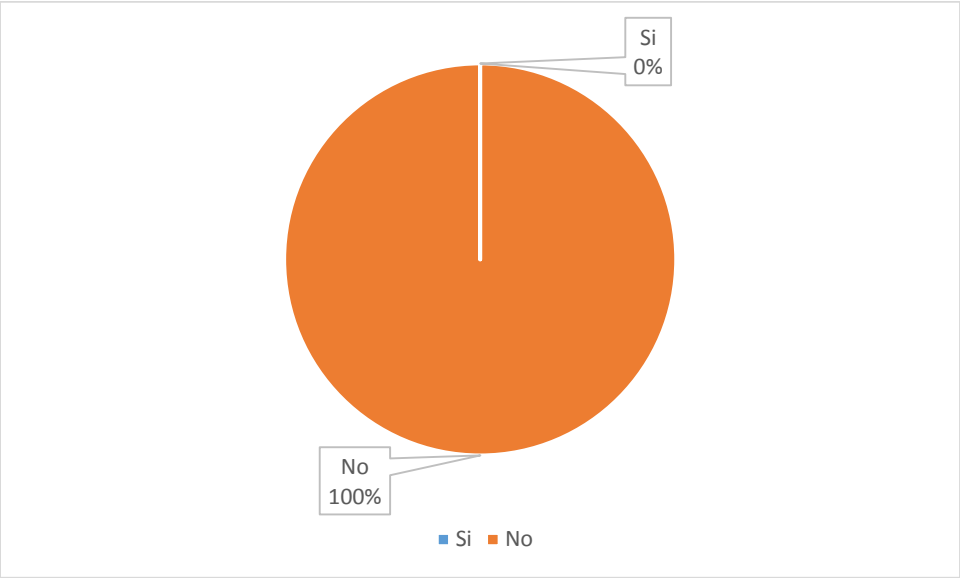

Gráfico 25. Pregunta No. 25

Análisis 25: En concordancia con la respuesta 24, el total de las encuestadas carece de procedimientos para el manejo de la información según su clasificación.

Recomendación 25: La organización debe documentar procedimientos que indiquen el adecuado manejo de la información según su clasificación.

Manejo de medios

Objetivo: Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de información almacenada en medios.

Pregunta No. 26

¿Existen procedimientos para la gestión de medios removibles en concordancia con la clasificación de información?

Objetivo 26: Conocer sobre la existencia de procedimientos para la gestión de manejo de medios removibles según el esquema de clasificación adoptado por la organización

Alternativa	Frecuencia	Porcentaje
Si	**1**	10%
No	**9**	90%
Total	10	100%

Tabla 31. Pregunta No. 26

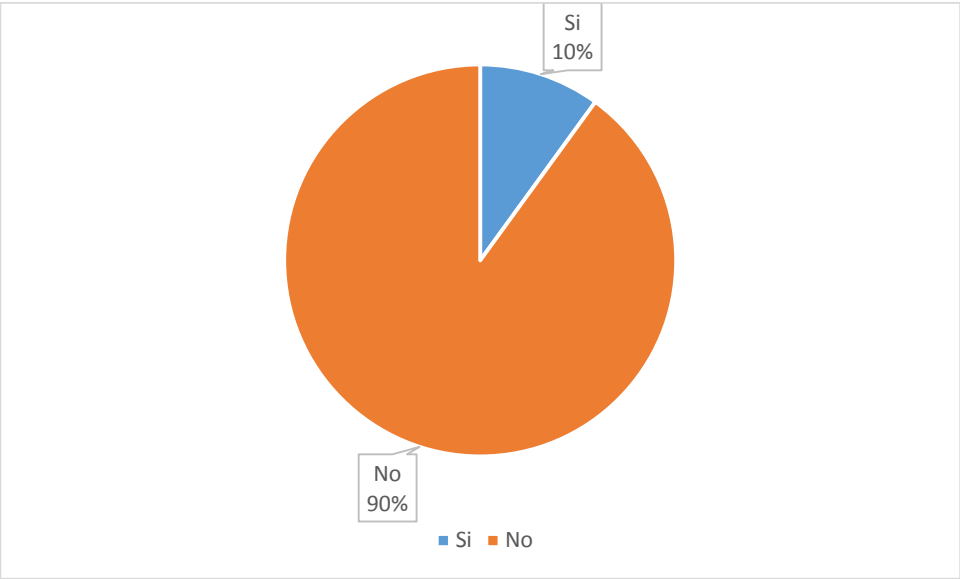

Gráfico 26. Pregunta No. 26

Análisis 26: Solamente el 10% de las empresas encuestadas manifiesta poseer procedimientos que ayuden a la gestión de medios removibles no obstante no se toma en cuenta el tipo de información almacenada en dichos medios.

Recomendación 26: Se debería establecer procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación de la información que adopte la organización.

Parte VI: Control de acceso

Requerimiento del negocio del control de acceso

Objetivos: Limitar el acceso a la información y a instalaciones de procesamiento de la información.

Pregunta No. 27

¿Cuenta con una política de control de acceso qué determine el acceso a la información y a instalaciones de procesamiento de la información?

Objetivo 27: Conocer si existe el establecimiento y documentación de una política para determinar el acceso a la información y a instalaciones de procesamiento de la misma

Alternativa	Frecuencia	Porcentaje
Si	**4**	40%
No	**6**	60%
Total	10	100%

Tabla 32. Pregunta No. 27

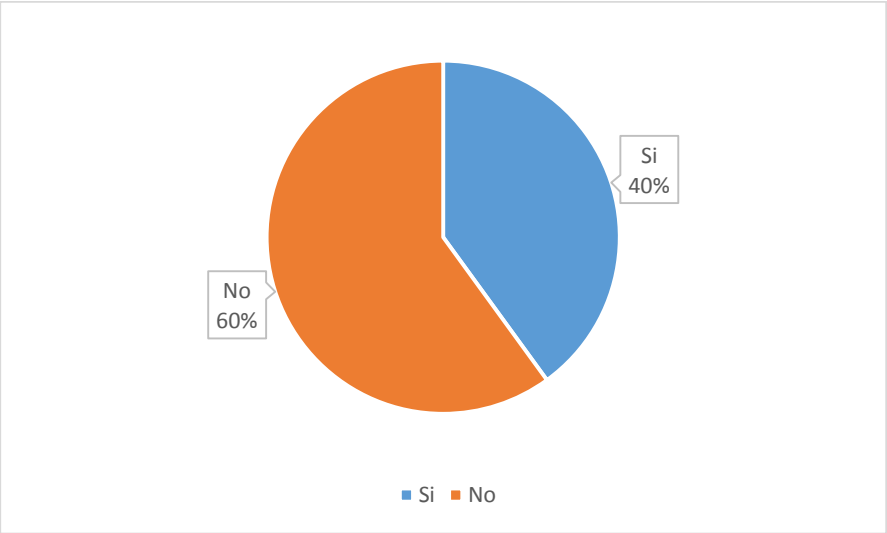

Gráfico 27. Pregunta No. 27

Análisis 27: Analizando los resultados de las empresas, solamente el 40% posee controles de acceso a la información, mientras que el resto no cuentan con ningún tipo de medida que restrinja el acceso, esta situación genera un alto grado de riesgo para la confidencialidad e integridad de la misma.

Recomendación 27: La organización debe establecer, documentar y autorizar una política de control de acceso que establezca las reglas para acceder y las medidas de seguridad para acceder a la información y a los lugares de procesamiento de información según las necesidades de seguridad de la organización.

Pregunta No. 28

¿Se provee a los usuarios únicamente los accesos autorizados?

Objetivo 28: Identificar si el acceso otorgado a los usuarios es únicamente el requerido según sus obligaciones

Alternativa	Frecuencia	Porcentaje
Si	**6**	60%
No	**4**	40%
Total	10	100%

Tabla 33. Pregunta No. 28

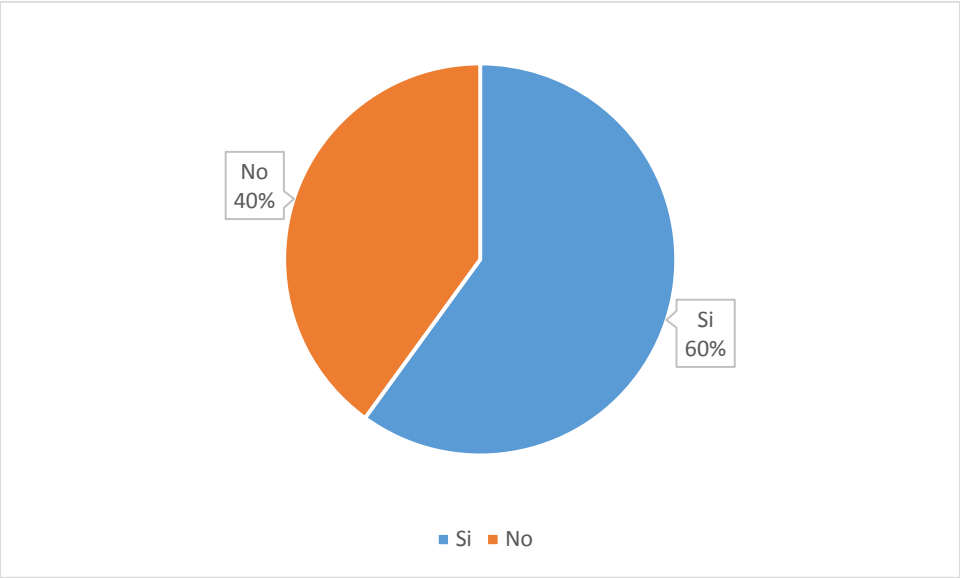

Gráfico 28. Pregunta No. 28

Análisis 28: Se puede observar que el 60% de casos, la organización brinda a los empleados únicamente los accesos requeridos de acuerdo a sus funciones y obligaciones.

Recomendación 28: La dirección debe asegurarse que el acceso provisto a los empleados para la realización de sus tareas esté acorde con las responsabilidades y funciones de su cargo.

Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.

Gestión del acceso de usuarios

Objetivo: Asegurar el acceso autorizado a los usuarios y prevenir el acceso no autorizado a los sistemas de información

Pregunta No. 29

¿Cuenta con un procedimiento para la creación y anulación de credenciales de usuarios?

Objetivo 29: Determinar si se cuenta con un procedimiento formal para la creación y anulación de credenciales de usuarios

Alternativa	Frecuencia	Porcentaje
Si	**5**	50%
No	**5**	50%
Total	10	100%

Tabla 34. Pregunta No. 29

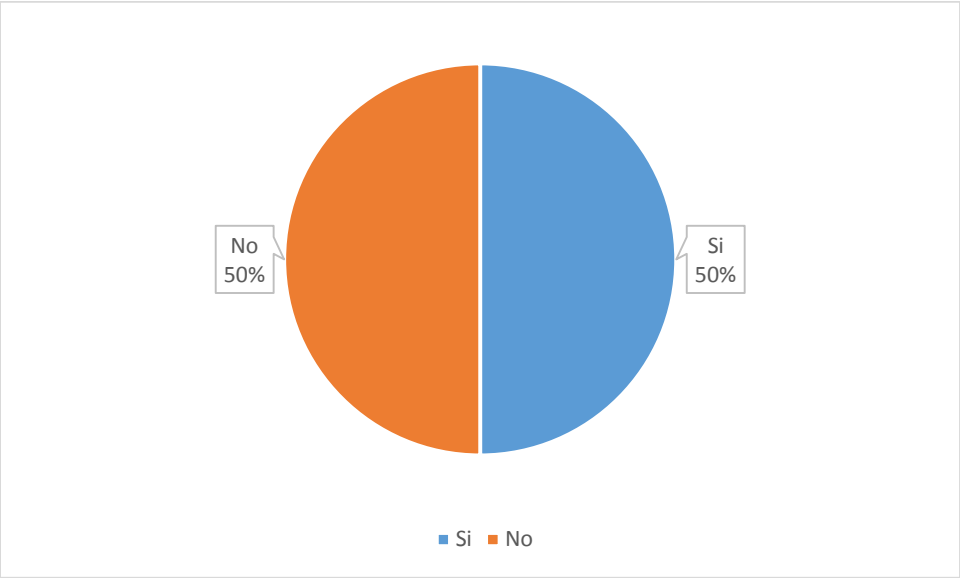

Gráfico 29. Pregunta No. 29

Análisis 29: Existe una paridad entre las empresas que cuenta con un procedimiento para la creación y anulación de credenciales de usuarios y las que no lo poseen. Esta situación podría generar una pérdida de control en los accesos a los sistemas y posibles eventos que se generen en ellos, afectando la integridad y confidencialidad de la información.

Recomendación 29: Debe existir un procedimiento para la alta y baja de usuarios para el acceso a los sistemas de información.

Pregunta No. 30

¿Existe un proceso para la provisión de derechos de acceso a los usuarios y la gestión de privilegios?

Objetivo 30: Identificar la existencia de algún proceso formal para el aprovisionamiento de derechos de acceso a los usuarios

Alternativa	Frecuencia	Porcentaje
Si	**3**	30%
No	**7**	70%
Total	10	100%

Tabla 35. Pregunta No. 30

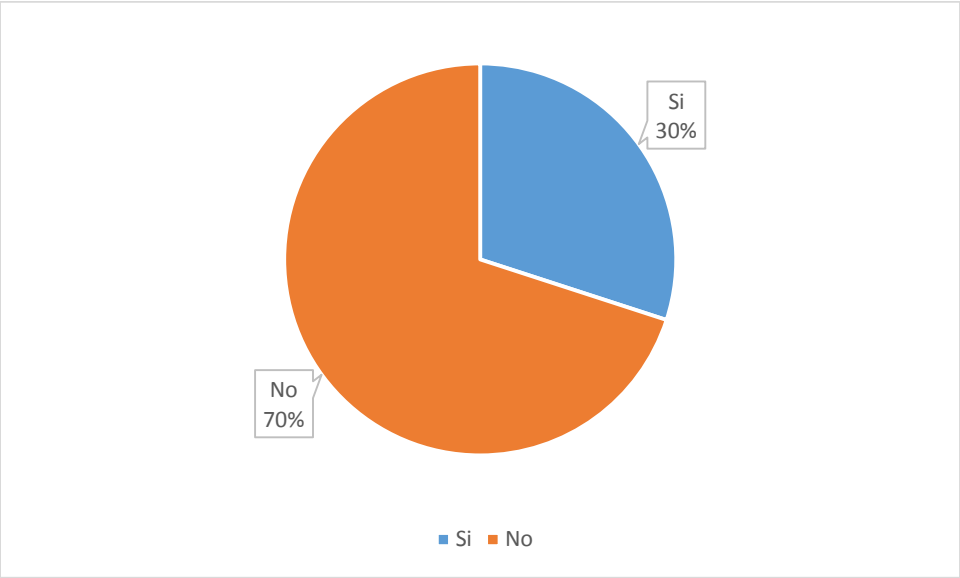

Gráfico 30. Pregunta No. 30

Análisis 30: Los resultados muestran que de las encuestas encuestadas un porcentaje alto no posee procedimiento de formal para el aprovisionamiento de derechos de acceso a los usuarios. Esta situación podría ocasionar una falta de control tanto para las solicitudes de creación para la gestión de accesos existentes.

Recomendación 30: La dirección debe asegurarse que la provisión y gestión de derechos de acceso a los usuarios se realice de forma controlada a través de un procedimiento formal.

Pregunta No. 31

¿Se realizan revisiones periódicas a los derechos de acceso de los usuarios?

Objetivo 31: Conocer si se realizan revisiones periódicas de usuarios y sus privilegios

Alternativa	Frecuencia	Porcentaje
Si	**0**	0%
No	**10**	100%
Total	10	100%

Tabla 36. Pregunta No. 31

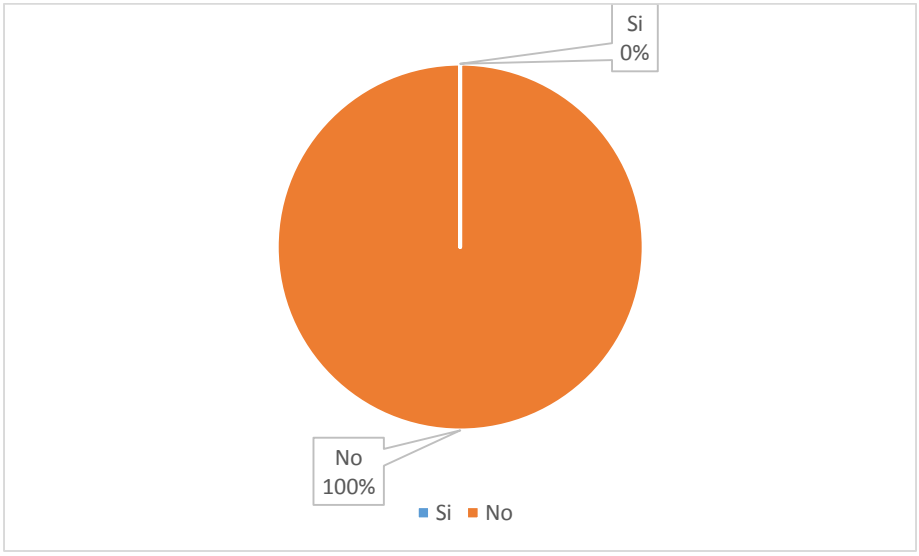

Gráfico 31. Pregunta No. 31

Análisis 31: El 100% de los casos revelaron que no realizan revisiones periódicas a los derechos de acceso de los usuarios. Esta situación puede llevar a generar un riesgo de confidencialidad e integridad de la información ya que podrían existir accesos no autorizados que no están acorde a los requisitos de seguridad de la organización.

Recomendación 31: Deben realizarse revisiones periódicas a la estructura de accesos y privilegios de usuarios en los sistemas de información en la organización.

Pregunta No. 32

¿Los derechos de acceso son removidos dada la terminación de contrato o ajustados cuando se dé un cambio?

Objetivo 32: Determinar si los accesos de usuarios son removidos o ajustados, una vez terminada la relación contractual entre el empleado y la empresa o si existen cambios en funciones de los mismos.

Alternativa	Frecuencia	Porcentaje
Si	**5**	50%
No	**5**	50%
Total	10	100%

Tabla 37. Pregunta No. 32

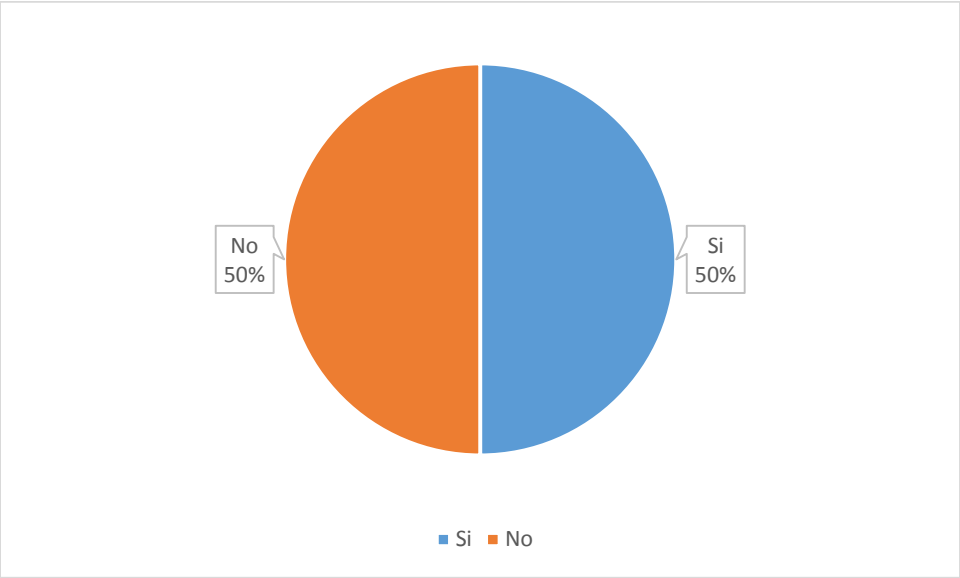

Gráfico 32. Pregunta No. 32

Análisis 32: Existe una igualdad en los resultados obtenidos, el 50% de las empresas manifiestan que dada la terminación de la relación contractual entre el empleado y la empresa o en casos que existan cambios internos, se realiza remoción o cambio de accesos. En el caso de las empresas que no lo realizan, existe una mayor probabilidad de generarse descontrol en la gestión de accesos para personal retirado o para empleados que por sus funciones actuales deben poseer un rol diferente en el acceso a los sistemas.

Recomendación 32: Se debe gestionar el control de bajas de usuarios en los sistemas, con base a sus funciones o estado actual del personal.

Responsabilidad del usuario

Objetivo: Hacer responsables a los usuarios por salvaguardar su información de autenticación

Pregunta No. 33

¿La organización requiere a los empleados hacer buen uso de la información de autenticación secreta (credenciales de acceso)?

Objetivo 33: Determinar si se requiere a los empleados seguir las prácticas de la organización en el uso de la información de autenticación secreta.

Alternativa	Frecuencia	Porcentaje
Si	**5**	50%
No	**5**	50%
Total	10	100%

Tabla 38. Pregunta No. 33

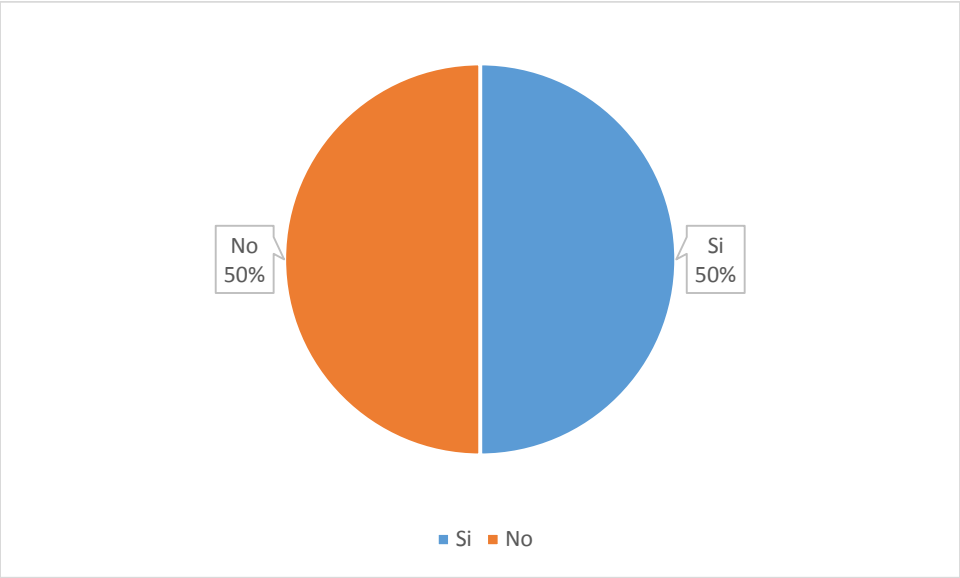

Gráfico 33. Pregunta No. 33

Análisis 33: La información obtenida refleja igual porcentaje para las organizaciones en las cuales se requiere al empleado dar seguimiento a las prácticas para hacer buen uso de la información de autenticación secreta como para las organizaciones que no lo requieren. Una falta de comprensión de la responsabilidad podría generar en los empleados un uso indebido de la información comprometiendo la seguridad de la misma.

Recomendación 33: La dirección debe exigir a los empleados el cumplimiento de las buenas prácticas de la organización para el uso de la información de autenticación secreta y asegurarse que cuenta con medidas para generar una adecuada segregación de accesos.

Control de acceso a sistemas y aplicaciones

Objetivo: Prevenir el acceso no autorizado a sistemas y aplicaciones

Pregunta No. 34

¿Los accesos a la información y a las funcionalidades de los sistemas informáticos están restringidos por niveles de acceso?

Objetivo 34:

Determinar si se implementan controles de seguridad para impedir el acceso no autorizado a la información mantenida por los sistemas de las aplicaciones.

Alternativa	Frecuencia	Porcentaje
Si	**7**	70%
No	**3**	30%
Total	10	100%

Tabla 39. Pregunta No. 34

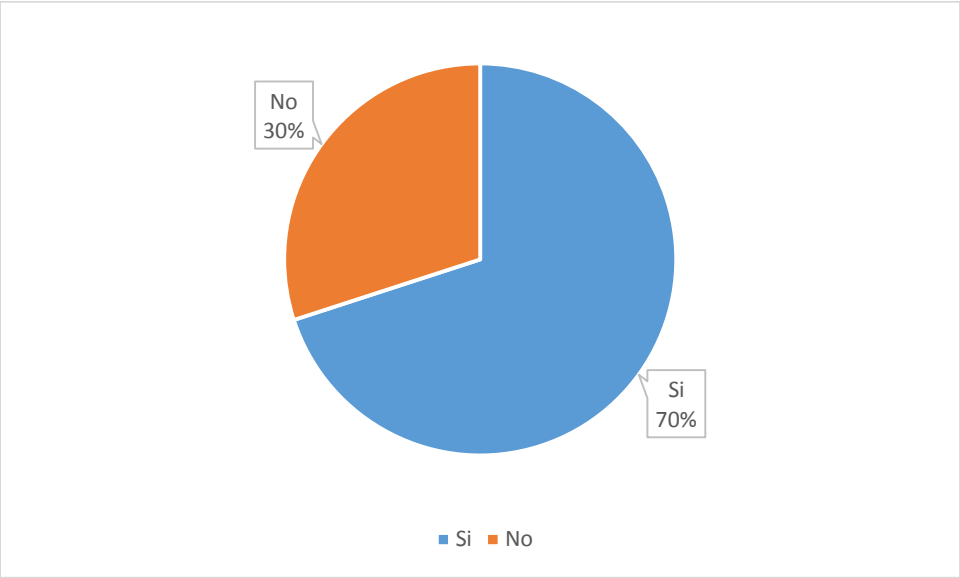

Gráfico 34. Pregunta No. 34

Análisis 34: Si bien, las PYMES dan cumplimiento en un 70% en cuanto a la implementación de medidas para limitar los niveles de acceso a la información, el 30% no poseen restricción de acceso a los sistemas independientemente de las funciones realizadas de cada empleado.

Recomendación 34: La dirección debería implementar un procedimiento donde se establezca los accesos de usuarios basados en roles, según las funciones de cada empleado.

Pregunta No. 35

¿Los sistemas y aplicaciones cuentan con funcionalidad de inicio seguro a través de credenciales de accesos?

Objetivo 35:

Conocer si la organización controla el acceso a sistemas de información a través de credenciales de acceso

Alternativa	Frecuencia	Porcentaje
Si	**8**	80%
No	**2**	20%
Total	10	100%

Tabla 40. Pregunta No. 35

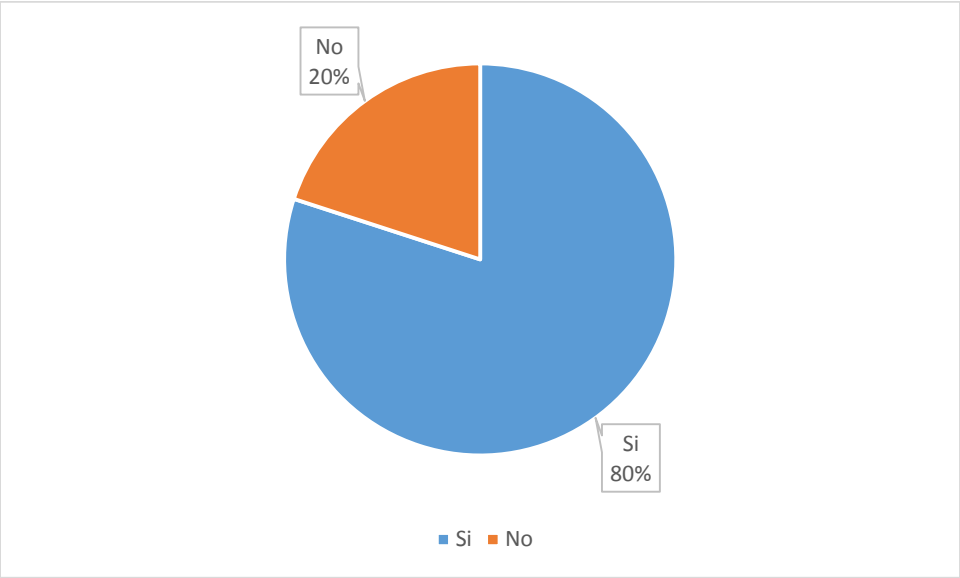

Gráfico 35. Pregunta No. 35

Análisis 35: De acuerdo a los resultados obtenidos el 80% de las empresas encuestadas manifiesta que la organización controla el acceso a sistemas de información a través de credenciales, el 20% de las empresas que manifestó no implementar ésta medida posee un alto riesgo de comprometer la información ya que cualquier usuario interno o externo podría acceder a la misma sin previa autorización.

Recomendación 35: Todos los sistemas de información deben implementar medidas de acceso a través de autenticación seguro.

Pregunta No. 36

¿La organización restringe y controla el uso de software no autorizado?

Objetivo 36:

Identificar si la organización restringe y controla el uso de software que podría comprometer la seguridad de la información

Alternativa	Frecuencia	Porcentaje
Si	**2**	20%
No	**8**	80%
Total	10	100%

Tabla 41. Pregunta No. 36

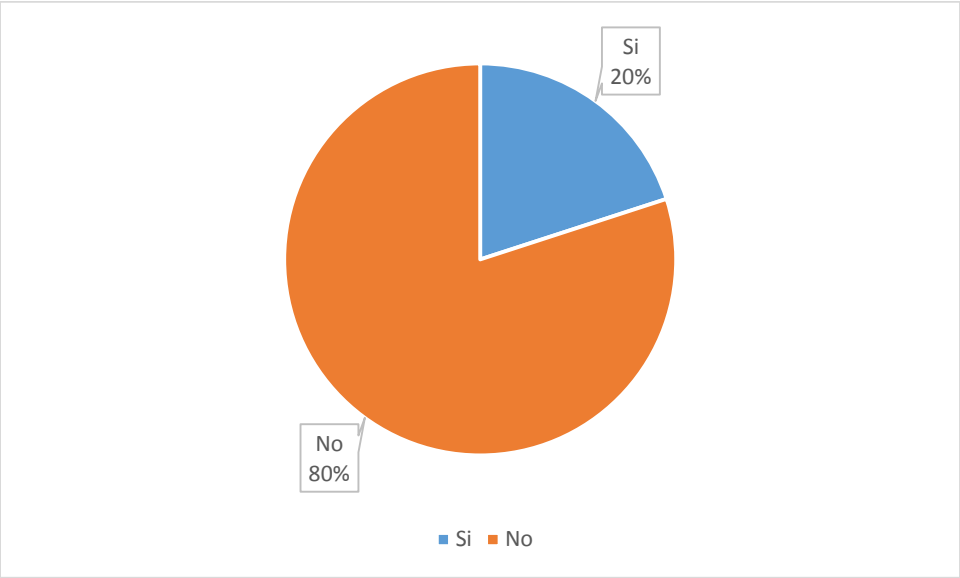

Gráfico 36. Pregunta No. 36

Análisis 36: Los resultados obtenidos demuestran que el 80% de las empresas encuestadas no cuentan con controles para restringir el uso de software no autorizado, el cual puede comprometer la seguridad de la información.

Recomendación 36: La organización de definir una política del uso de software donde se establezca las restricciones de la utilización de software no autorizado, además debe realizar revisiones periódicas para validar el cumplimiento de dicha política.

Pregunta No. 37

¿La organización restringe el acceso al código fuente de los sistemas?

Objetivo 37: Determinar si existen restricciones de acceso al código fuente de los programas.

Alternativa	Frecuencia	Porcentaje
Si	**3**	30%
No	**7**	70%
Total	10	100%

Tabla 42. Pregunta No. 37

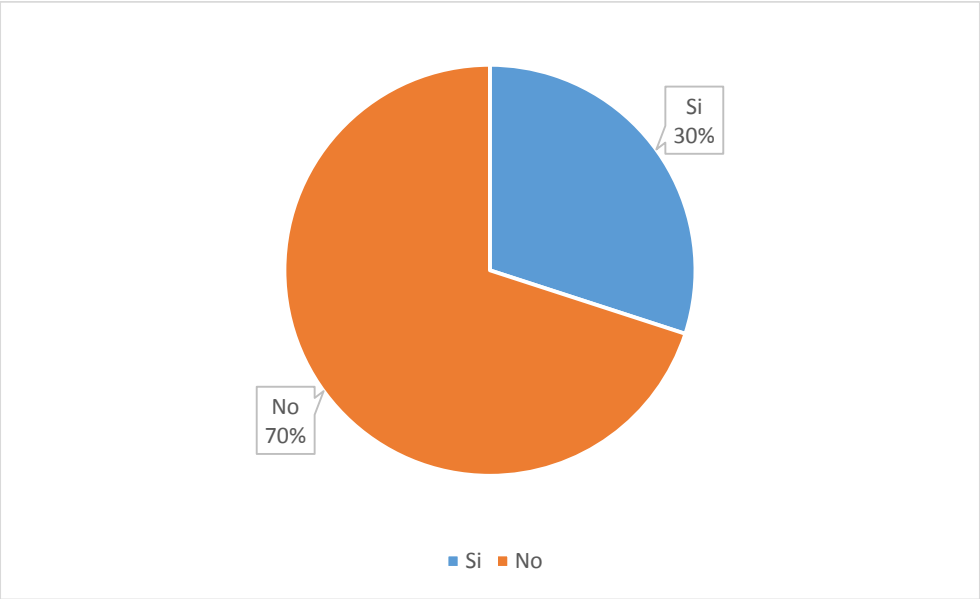

Gráfico 37. Pregunta No. 37

Análisis 37: En las PYME a pesar que no siempre se cuenta con los códigos fuente de los programas, el 30% manifestó que se implementan medidas para controlar el acceso dicho códigos, el resto de las empresas que no implementan medidas lo hacen por desconocimiento o por no poseer el código fuente de los programas.

Recomendación 37: En el caso que la organización cuente con el código fuente de algún programa, ésta debe establecer e implementar controles para restringir el acceso a dicho código.

Parte VII: Criptografía. Controles

Objetivo: Asegurar el apropiado y efectivo uso de la criptografía para proteger la confidencialidad, autenticidad, y/o integridad de la información

Pregunta No. 38

¿Existe un documento que defina el uso de controles criptográficos para la protección de la información?

Objetivo 38:

Determinar si existe un documento que defina los controles que deben implementarse para proteger la confidencialidad e integridad de la información.

Alternativa	Frecuencia	Porcentaje
Si	**0**	0%
No	**10**	100%
Total	10	100%

Tabla 43. Pregunta No. 38

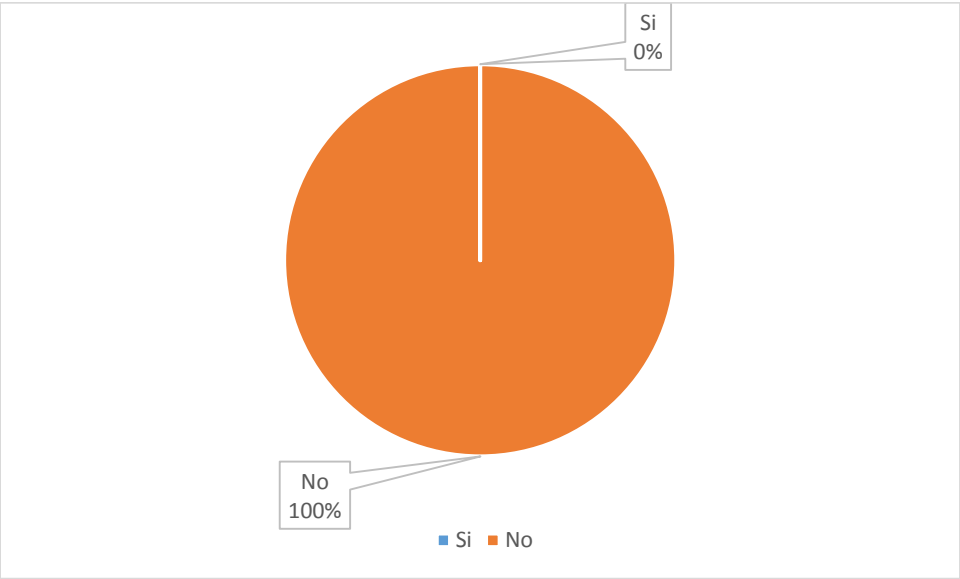

Gráfico 38. Pregunta No. 38

Análisis 38: El 100% de las empresas manifestó que no cuentan con ningún control criptográfico para proteger la confidencialidad e integridad de la información.

Recomendación 38: La organización debería establecer medidas para el cifrado de la información sensible.

Parte VIII: Seguridad física y ambiental. Áreas seguras

Objetivo: Prevenir el acceso físico no autorizado, daño e interferencia a las instalaciones de procesamiento de la información y a la información de la organización

Pregunta No. 39

¿La organización ha definido perímetros de seguridad para controlar el acceso a áreas que contienen información sensitiva o crítica?

Objetivo 39:

Determinar si la organización restringe el acceso a áreas de trabajo donde se procesa o resguarda información sensitiva o crítica.

Alternativa	Frecuencia	Porcentaje
Si	**7**	70%
No	**3**	30%
Total	10	100%

Tabla 44. Pregunta No. 39

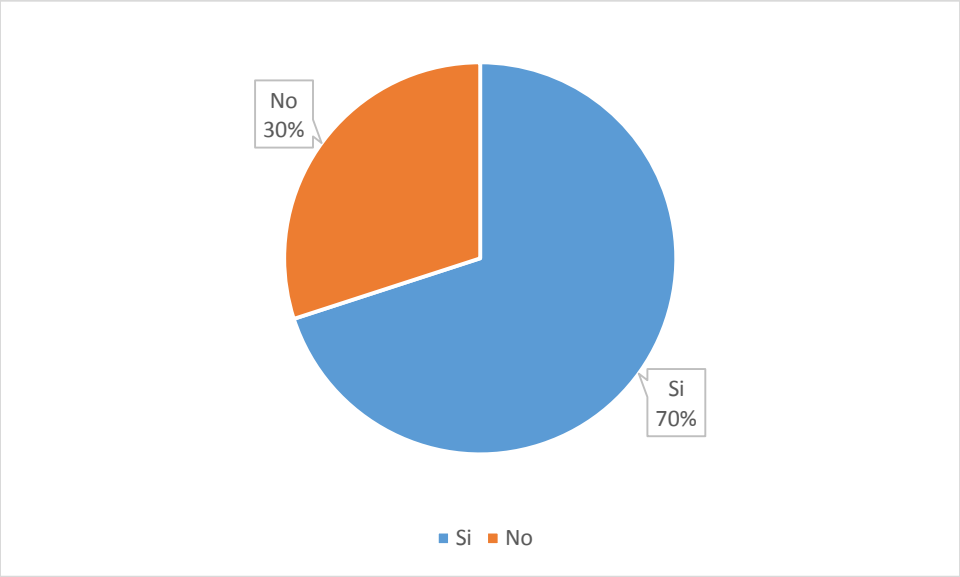

Gráfico 39. Pregunta No. 39

Análisis 39: A pesar que un alto porcentaje de las PYME mencionó que implementan medidas para restringir el acceso a áreas que tienen información sensible o crítica, las implementaciones de éstas medidas no necesariamente brindan un grado de seguridad aceptable

Recomendación 39: La organización debe restringir el acceso a áreas que tienen información sensible o crítica mediante controles adecuados.

Pregunta No. 40

¿El acceso a las áreas seguras está protegidas por controles de entrada para asegurar el ingreso al personal autorizado?

Objetivo 40:

Identificar si la organización implementa controles para restringir el acceso a las áreas donde se procesa o resguarda información sensitiva o crítica.

Alternativa	Frecuencia	Porcentaje
Si	**2**	20%
No	**8**	80%
No se	**0**	0%
Total	10	100%

Tabla 45. Pregunta No. 40

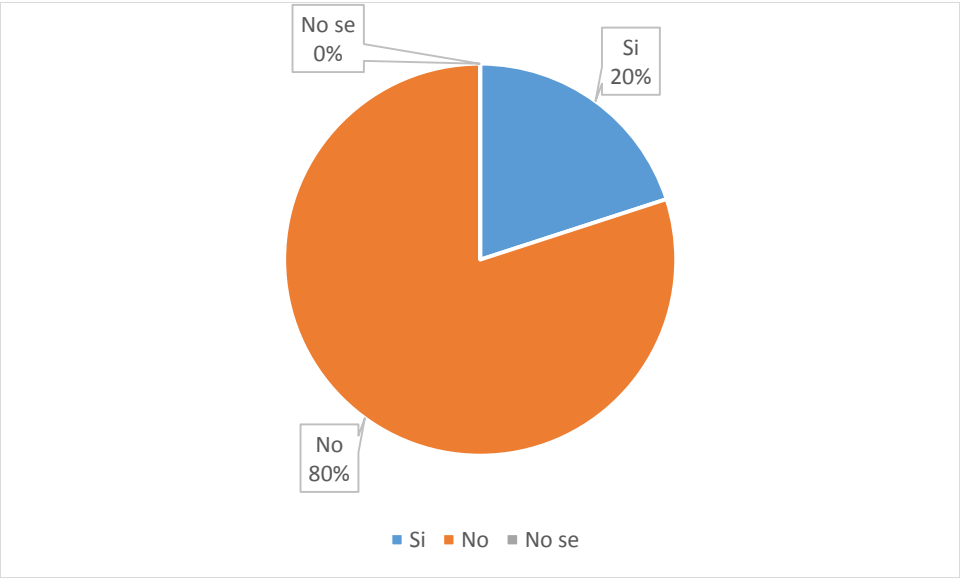

Gráfico 40. Pregunta No. 40

Análisis 40: A pesar que en la pregunta 39 el 70% de las empresas encuestadas mencionaron que poseen perímetros para controlar el acceso a áreas que poseen información sensible, solamente el 20% del total de las empresas posee controles de acceso para dichos perímetros.

Recomendación: 40: Se debe implementar medidas para garantizar acceso controlado a las áreas que procesen y resguarden información sensible o crítica para la organización.

Pregunta No. 41

¿Las instalaciones donde se encuentran equipos críticos cuentan con medidas de seguridad físicas?

Objetivo 41:

Conocer si la organización ha implementado un sistema de seguridad física en las áreas donde se encuentran equipos que procesan o almacena información.

Alternativa	Frecuencia	Porcentaje
Si	**5**	50%
No	**5**	50%
No se	**0**	0%
Total	10	100%

Tabla 46. Pregunta No. 41

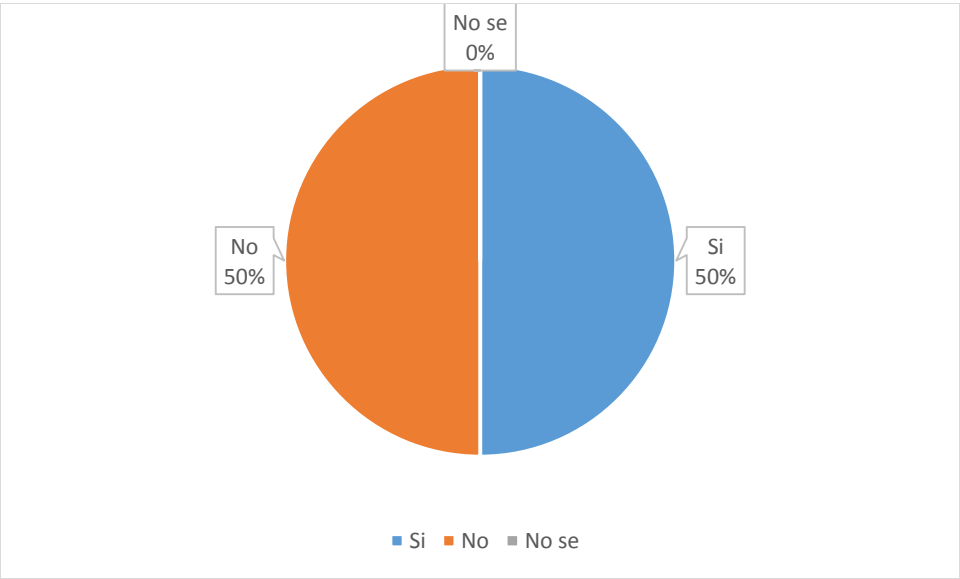

Gráfico 41. Pregunta No. 41

Análisis 41: De acuerdo a los resultados obtenidos, existe una paridad en las empresas que implementan alguna medida de seguridad física para las áreas donde se encuentran equipos críticos, para el 50% de las empresas que no implementan medidas se puede considerar como un punto vulnerable ante incidente que atenten contra la confidencialidad, disponibilidad e integridad de la información.

Recomendación 41: Debe implementar las medidas físicas para la protección de los equipos considerados críticos para la organización.

Equipo

Objetivo: Prevenir la pérdida, daño o robo o exposición de los activos y la interrupción de las operaciones de la organización

Pregunta No. 42

¿El equipo se encuentra ubicado y protegido de accesos no autorizados?

Objetivo 42:

Determinar si la organización implementa medidas para reducir el riesgo de oportunidades de acceso no autorizado a equipos.

Alternativa	Frecuencia	Porcentaje
Si	**8**	80%
No	**2**	20%
No se	**0**	0%
Total	10	100%

Tabla 47. Pregunta No. 42

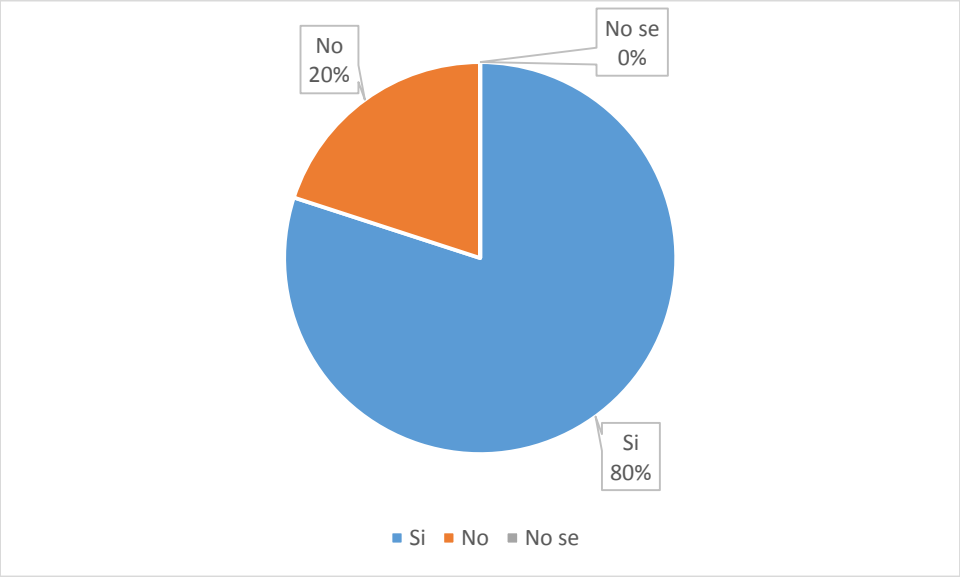

Gráfico 42. Pregunta No. 42

Análisis 42: El 80% de las empresas encuestadas manifiestan que el equipo se encuentra ubicado físicamente en espacios de acceso restringidos limitando los accesos únicamente al personal autorizado.

Recomendación 42: La organización debe garantizar que los equipos se encuentren ubicados físicamente en lugares con acceso restringido.

Pregunta No. 43

¿Los equipos de cómputo están protegidos contra fallas de energía?

Objetivo 43:

Identificar si se implementa medidas en los equipos de cómputo para asegurar la disponibilidad de la información y la continuidad de las operaciones.

Alternativa	Frecuencia	Porcentaje
Si	**10**	100%
No	**0**	0%
No se	**0**	0%
Total	10	100%

Tabla 48. Pregunta No. 43

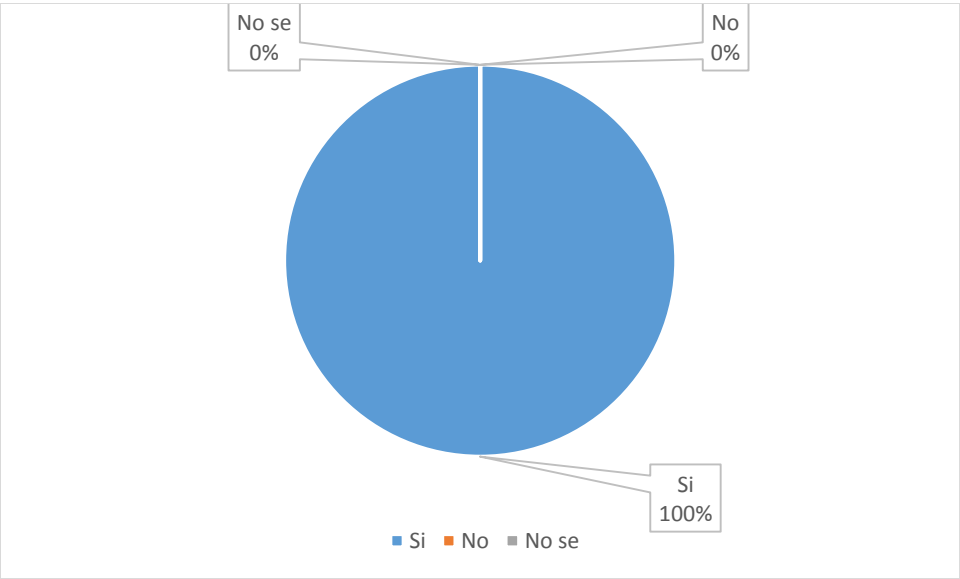

Gráfico 43. Pregunta No. 43

Análisis 43: El total de las empresas manifiestan que los equipos están protegidos contra fallas de energía eléctrica. Garantizando la disponibilidad de la información.

Recomendación 44: Las organizaciones deben asegurarse que los equipos de cómputo cuenten con protección antes fallas de energía eléctrica.

Pregunta No. 44

¿Se cuenta con un cableado eléctrico y de telecomunicaciones protegido de intercepción, interferencia o daño?

Objetivo 44:

Determinar si los cables eléctricos y de telecomunicaciones que transportan datos o apoyan en los servicios de información se encuentran debidamente protegidos contra la intercepción, interferencia o posibles daños.

Alternativa	Frecuencia	Porcentaje
Si	**6**	60%
No	**2**	20%
No se	**2**	20%
Total	10	100%

Tabla 49. Pregunta No. 44

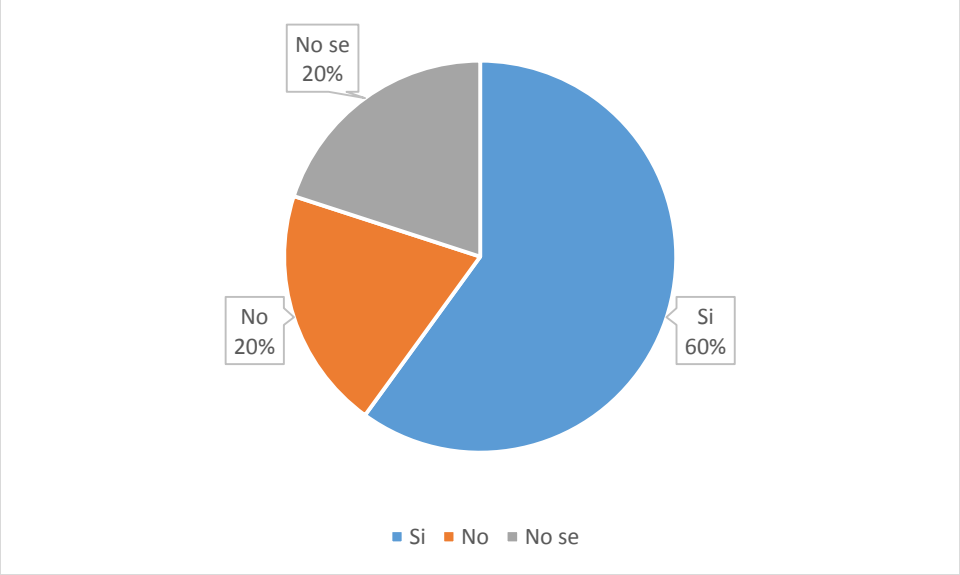

Gráfico 44. Pregunta No. 44

Análisis 44: De acuerdo a los resultados obtenidos el 40% de las empresas manifiestan que no poseen o no tienen conocimiento sobre medidas de protección para el cable eléctrico y de comunicaciones. El resto mencionaron que si cuentan con cableados eléctrico y de comunicación protegidos.

Recomendación 44: La organización debe garantizar que el cableado tanto eléctrico como de comunicaciones cuente con la distribución y protección adecuada.

Pregunta No. 45

¿Se cuenta con un plan de mantenimiento de equipo informático?

Objetivo 45:

Conocer si la organización ha establecido un plan de mantenimiento de equipo informático con el objeto de garantizar su disponibilidad e integridad continuas.

Alternativa	Frecuencia	Porcentaje
Si	**2**	20%
No	**8**	80%
No se	**0**	0%
Total	10	100%

Tabla 50. Pregunta No. 45

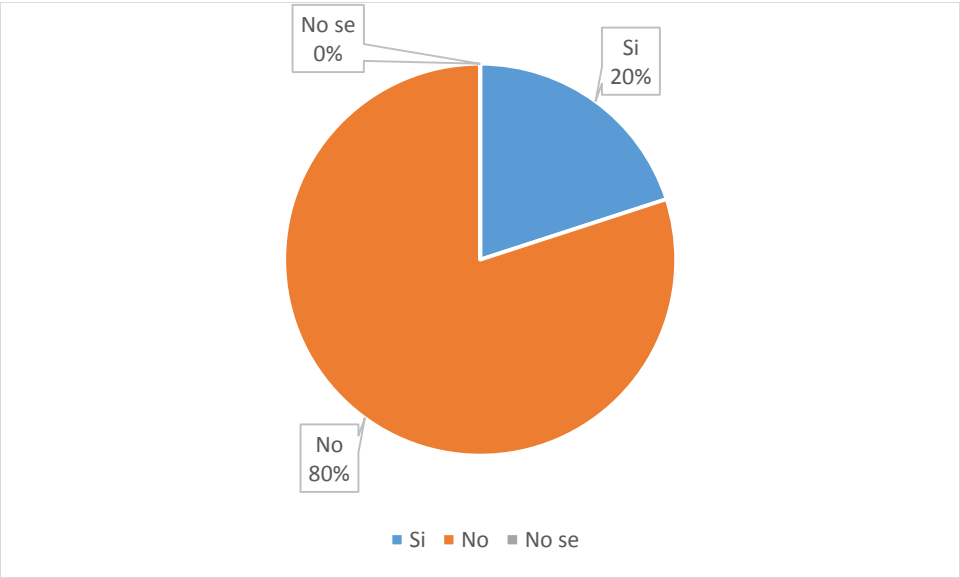

Gráfico 45. Pregunta No. 45

Análisis 45: Los resultados indican que las empresas no están concientes de la importancia de brindar un mantenimiento periódico de los equipos informáticos, situación que afecta la disponibilidad de la información y genera un riesgo de daño de equipo. Únicamente el 20% de las empresas cuentan con un plan de mantenimiento.

Recomendación 45: Las organizaciones deben contar con un plan de mantenimiento de equipo informático que se ejecute de forma periódica.

Pregunta No. 46

¿Se cuenta con un procedimiento para el retiro de equipo de las instalaciones?

Objetivo 46:

Determinar si existe un documento que defina el procedimiento a seguir para evitar el retiro de equipos, información o software sin previa autorización.

Alternativa	Frecuencia	Porcentaje
Si	**4**	40%
No	**6**	60%
No se	**0**	0%
Total	10	100%

Tabla 51. Pregunta No. 46

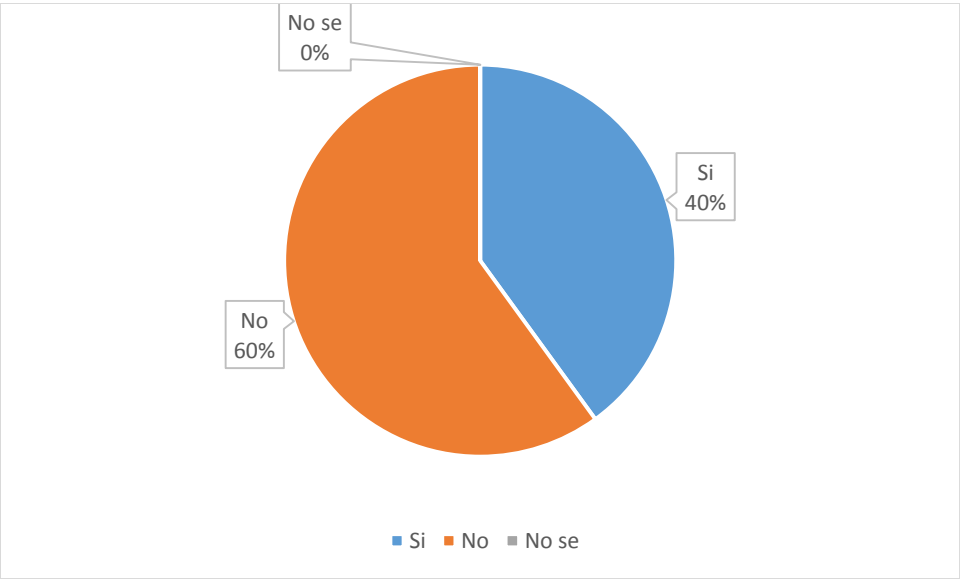

Gráfico 46. Pregunta No. 46

Análisis 46: De acuerdo a los resultados obtenidos, el 60% de las empresas encuestadas no posee un procedimiento para el retiro de equipo de las instalaciones, situación que podría afectar la pérdida de información contenida en los mismos.

Recomendación 46: La organización debe documentar e implementar un procedimiento que asegure un flujo de autorizaciones para el retiro de equipos de las instalaciones.

Pregunta No. 47

¿La organización cuenta con procedimientos para el borrado seguro de medios de almacenamiento para su utilización o descarte?

Objetivo 47:

Identificar si existen documentos donde se defina el procedimiento a seguir para para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización.

Alternativa	Frecuencia	Porcentaje
Si	**2**	20%
No	**8**	80%
No se	**0**	0%
Total	10	100%

Tabla 52. Pregunta No. 47

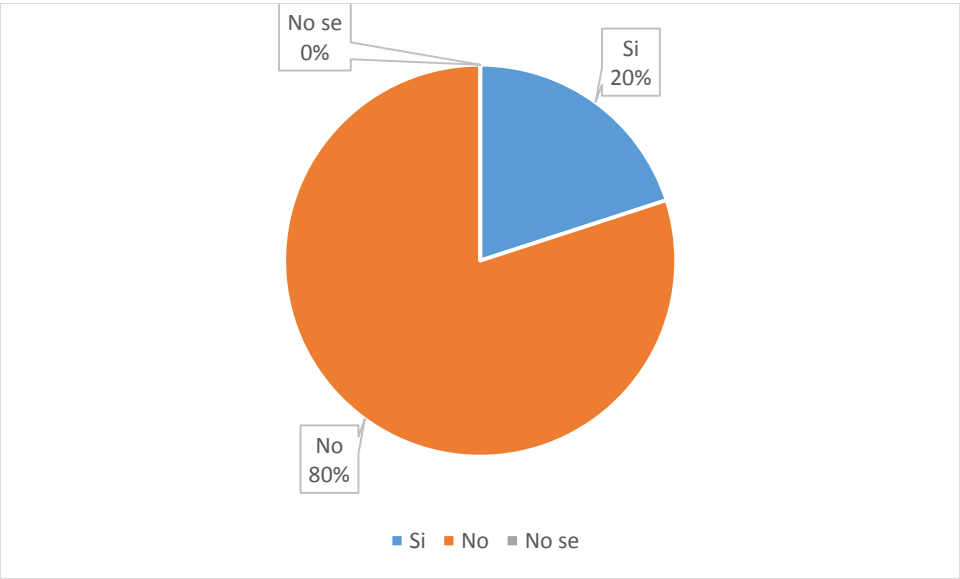

Gráfico 47. Pregunta No.47

Análisis 47: Es claro que la mayor parte de las empresas no cuenta con ningún tipo de procedimiento para el borrado seguro de medios de almacenamiento, situación que pudiese afectar la confidencialidad de la información contenida en éstos.

Recomendación 47: La organización debe definir un procedimiento que garantice la confidencialidad de la información a través de un borrado seguro de medios de almacenamiento para que éstos puedan ser reutilizados o descartados.

Pregunta No. 48

¿Los empleados se aseguran que los equipos desatendidos cuentan la protección adecuada (hurto)?

Objetivo 48:

Identificar si la organización implementa medidas de seguridad para asegurar que los equipos no supervisados cuentan con la protección adecuada.

Alternativa	Frecuencia	Porcentaje
Si	**2**	20%
No	**8**	80%
No se	**0**	0%
Total	10	100%

Tabla 53. Pregunta No. 48

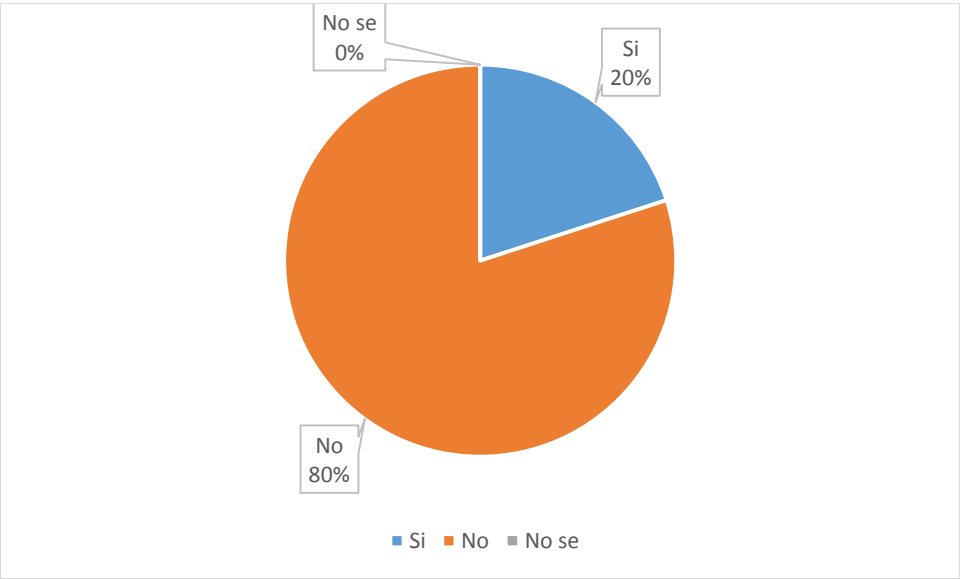

Gráfico 48. Pregunta No. 48

Análisis 48: Un alto porcentaje de las empresas encuestadas no implementan ningún tipo de medidas de seguridad para proteger los equipos desatendidos o no supervisados, mientras que el 20% implementa medidas que garantizan la protección tanto lógica como física.

Recomendación 48: La organización debe implementar medidas básicas de protección contra accesos no autorizados a equipos desatendidos o no supervisados.

Pregunta No. 49

¿Los equipos cuentan con bloqueo automático para proteger el acceso no autorizado?

Objetivo 49:

Conocer si la organización implementa controles para proteger la integridad de la información a través de la activación de restricción de acceso automático.

Alternativa	Frecuencia	Porcentaje
Si	5	50%
No	5	50%
No se	0	0%
Total	10	100%

Tabla 54. Pregunta No. 49

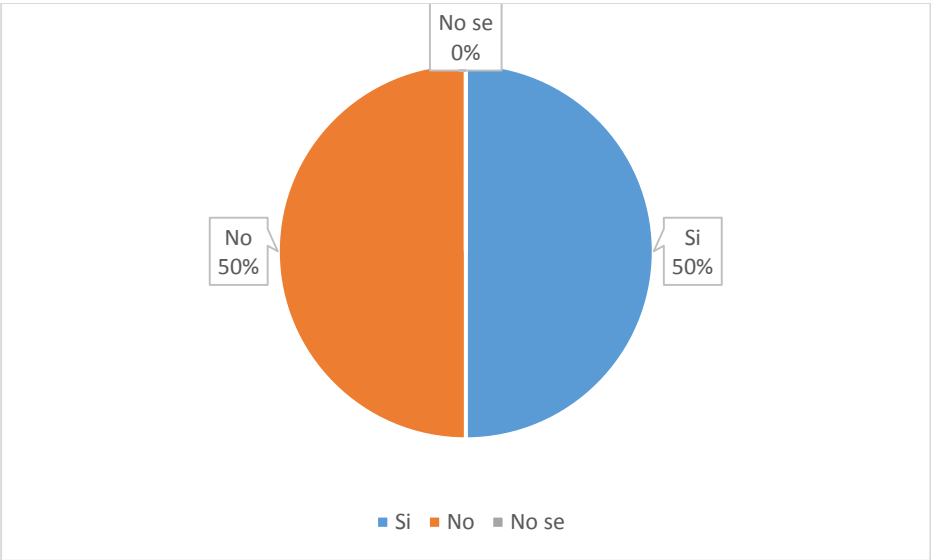

Gráfico 49. Pregunta No. 49

Análisis 49: Solamente el 50% de las empresas manifestaron tener implementados controles de bloqueo automático para proteger los accesos no autorizados a los equipos.

Recomendación 49: La dirección debe garantizar la confidencialidad de la información a través de la implementación de controles de bloqueo automático en los equipos.

Seguridad en las operaciones. Procedimientos y responsabilidades operacionales

Objetivo: Asegurar la operación correcta y segura de las instalaciones de procesamiento de información

Pregunta No. 50

¿Existen procedimientos de operación documentados y disponibles a los usuarios que los necesiten?

Objetivo 50: Determinar si la organización posee procedimientos de operación documentados y están accesibles para los usuarios que lo requieran.

Alternativa	Frecuencia	Porcentaje
Si	0	0%
No	10	100%
No se	0	0%
Total	**10**	**100%**

Tabla 55. Pregunta No. 50

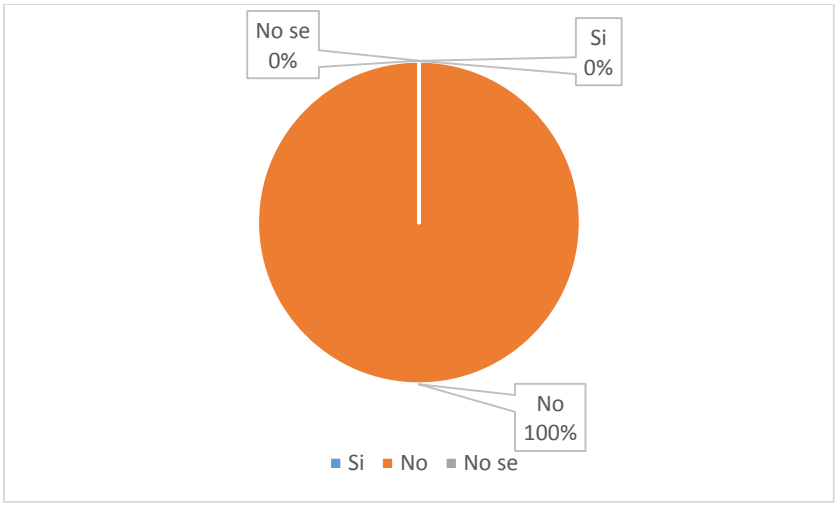

Gráfico 50. Pregunta No. 50

Análisis 50: El 100% de las empresas encuestadas manifestaron que no cuentan con procedimientos elaborados donde se especifiquen las actividades operacionales.

Recomendación 50: La organización debería elaborar, comunicar y publicar los procedimientos y responsabilidades operacionales.

Pregunta No. 51

¿Existe un proceso de aprobación para realizar cambios en sistemas de información?

Objetivo 51:

Determinar si existen controles de autorización sobre requerimientos de cambios en sistemas de información.

Alternativa	Frecuencia	Porcentaje
Si	1	10%
No	9	90%
No se	0	0%
Total	**10**	**100%**

Tabla 56. Pregunta No. 51

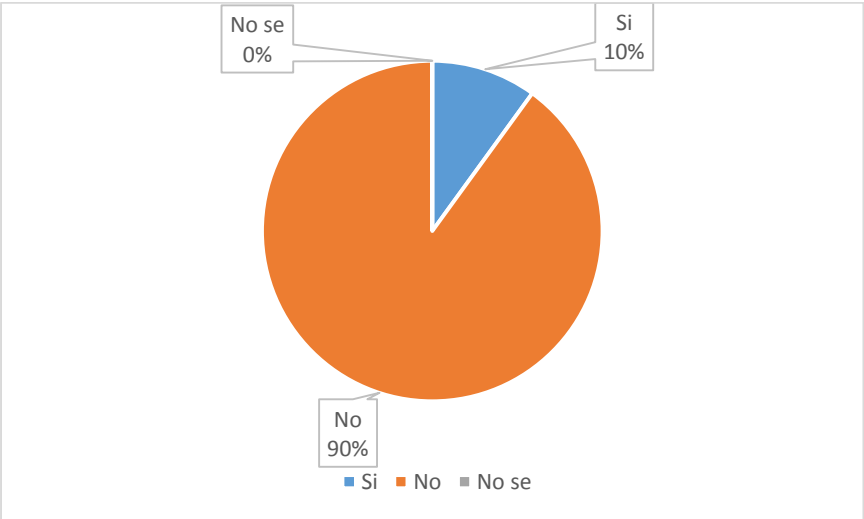

Gráfico 51. Pregunta No. 51

Análisis 51: La mayor parte de las empresas encuestadas mencionan que no cuentan con ningún proceso de aprobación para la realización de cambios en sistemas de información, solamente el 10% manifestó contar con procedimientos para gestionar dichos cambios. La ausencia de este control podría afectar la integridad de la información y la disponibilidad de los sistemas.

Recomendación 51: Se debe implementar un proceso de aprobación para gestionar los cambios en sistemas de información que garantice que los cambios requeridos cuentan con la autorización de la dirección.

Pregunta No. 52

¿Existe un monitoreo de optimización y disponibilidad de recursos para asegurar el desempeño requerido por los sistemas?

Objetivo 52:

Identificar si la organización realiza monitoreo periódico sobre el estado de los recursos informáticos para asegurar los requerimientos necesarios para mantener la disponibilidad de los sistemas de información.

Alternativa	Frecuencia	Porcentaje
Si	**1**	10%
No	**9**	90%
No se	**0**	0%
Total	**10**	**100%**

Tabla 57. Pregunta No. 52

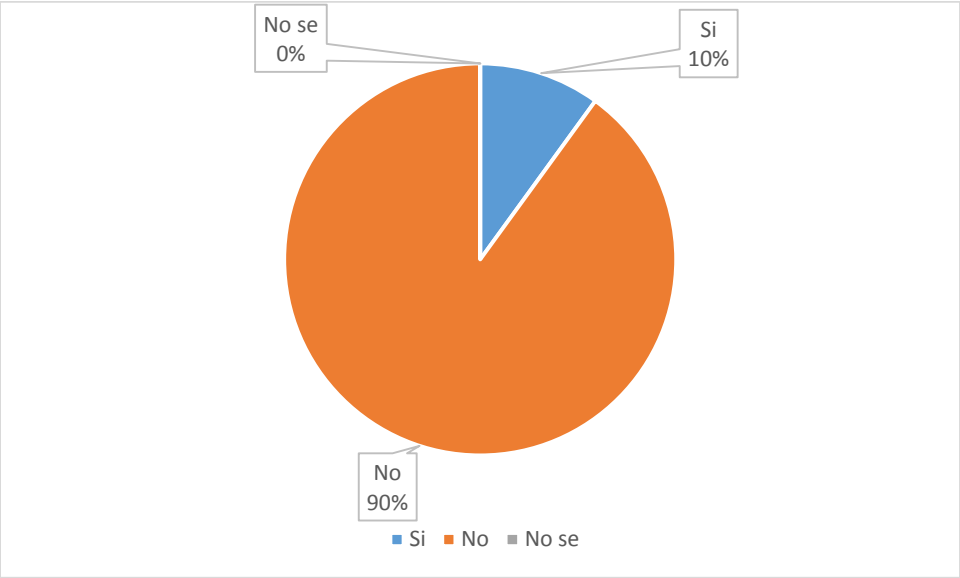

Gráfico 52. Pregunta No. 52

Análisis 52: Existe un alto porcentaje de empresas que no realizan monitoreo del estado de recursos. La ausencia de éste control podría afectar la disponibilidad de los sistemas de información.

Recomendación 52: La organización debería implementar un procedimiento de monitoreo periódico de recursos a fin de asegurar el desempeño requerido por los sistemas.

Pregunta No. 53

¿Existe una segregación de ambientes para los sistemas de información (ambiente de desarrollo, pruebas y producción)?

Objetivo 53:

Conocer si la organización implementa ambientes controlados para el desarrollo, pruebas y puesta en operación de sistemas de información.

Alternativa	Frecuencia	Porcentaje
Si	**2**	20%
No	**8**	80%
No se	**0**	0%
Total	**10**	**100%**

Tabla 58. Pregunta No. 53

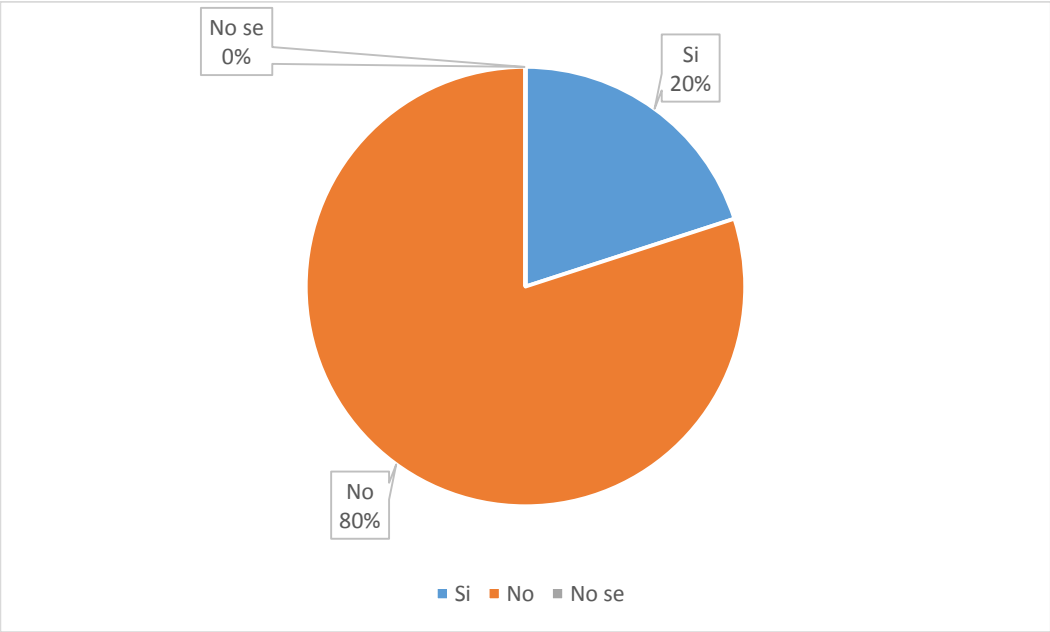

Gráfico 53. Pregunta No. 53

Análisis 53: Queda claro que la mayoría de las empresas encuestadas no cuentan con una debida segregación de ambientes para la distribución de los diferentes entornos de los sistemas de información. No obstante, no todas las empresas requieren el desarrollo interno de aplicaciones.

Recomendación 53: La organización debería poseer en los casos en que se requiera, entornos de ambiente separado para el desarrollo, prueba y producción de los sistemas de información.

Protección contra software malicioso

Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra software malicioso

Pregunta No. 54

¿Cuenta con un antivirus actualizado en cada uno de los equipos?

Objetivo 54:

Determinar si la organización implementa controles para la detección, prevención y recuperación de afectaciones de malware.

Alternativa	Frecuencia	Porcentaje
Si	**8**	80%
No	**1**	10%
No se	**1**	10%
Total	**10**	**100%**

Tabla 59. Pregunta No. 54

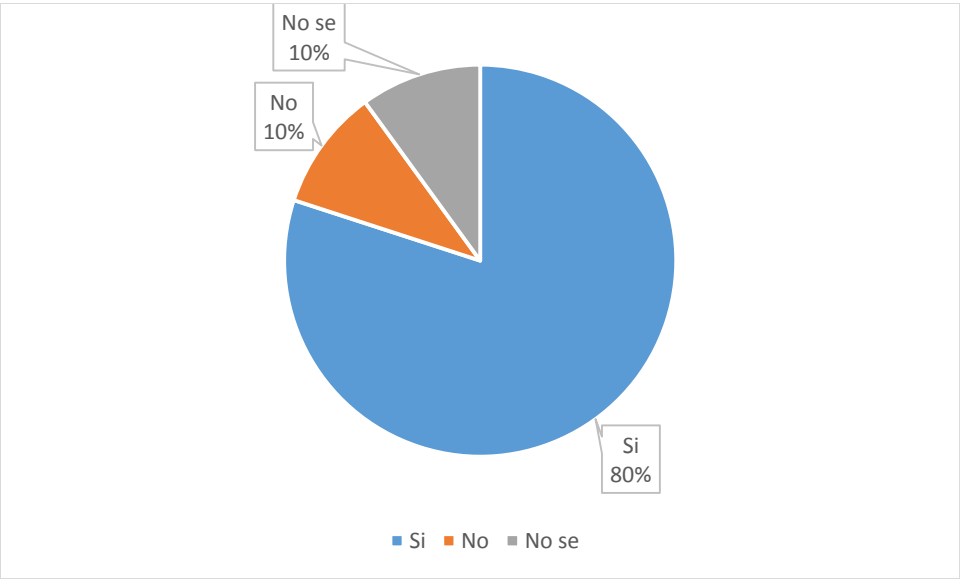

Gráfico 54. Pregunta No. 54

Análisis 54: Dados los resultados podemos observar que, en la mayoría de las empresas encuestadas, existe un grado de conciencia sobre la protección de los equipos a través del uso de software antivirus. La ausencia de ésta medida compromete la confidencialidad, integridad y disponibilidad de la información.

Recomendación 54: La dirección debe garantizar que los equipos de la organización cuentan con software antivirus y que la tarea de actualización de dicho software ha sido asignada.

Copias de seguridad

Objetivo: Proteger contra pérdida de datos

Pregunta No. 55

¿Cuenta con un procedimiento para realizar y probar copias de respaldo?

Objetivo 55:

Identificar si la organización implementa controles para realizar y probar regularmente copias seguridad de los sistemas de información.

Alternativa	Frecuencia	Porcentaje
Si	**2**	20%
No	**7**	70%
No se	**1**	10%
Total	10	100%

Tabla 60. Pregunta No. 55

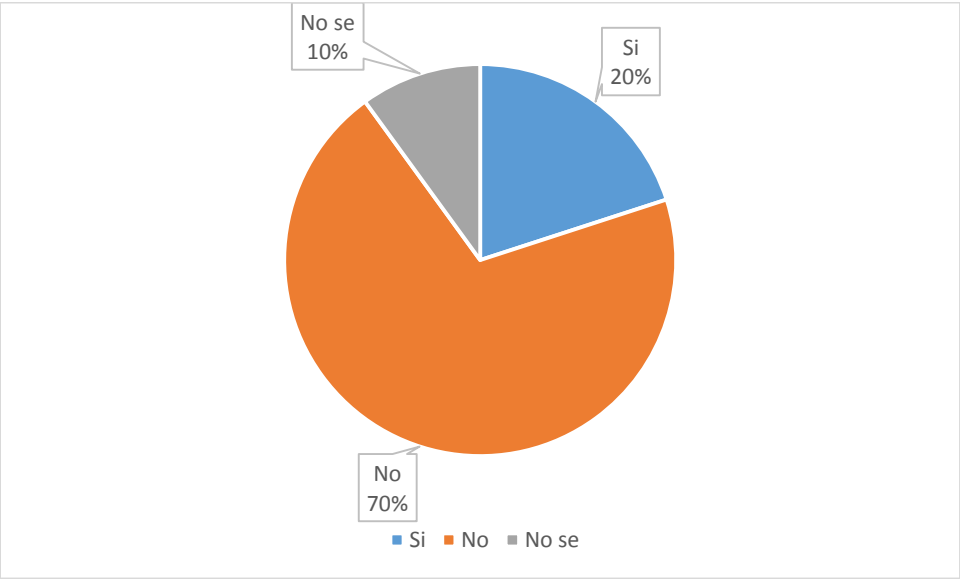

Gráfico 55. Pregunta No. 55

Análisis 55: El 70% de las empresas encuestadas manifiesta que no poseen procedimientos para realizar y probar copias de respaldo, mientras que un 10% manifestó desconocer si se cuenta con dichos procedimientos. Afectando la disponibilidad de la información.

Recomendación 55: La dirección debe asegurar que se cuenta con procedimientos para el respaldo y pruebas de restauración para la información que se considera crítica para la organización.

Registro y monitoreo

Objetivo: Proteger contra pérdida de datos

Pregunta No. 56

¿Los sistemas de información cuentan con pistas de auditoría de actividad de usuarios y administradores, monitoreadas y revisadas periódicamente?

Objetivo 56:

Conocer si la organización implementa controles para producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario.

Alternativa	Frecuencia	Porcentaje
Si	3	30%
No	7	70%
No se	0	0%
Total	**10**	**100%**

Tabla 61. Pregunta No. 56

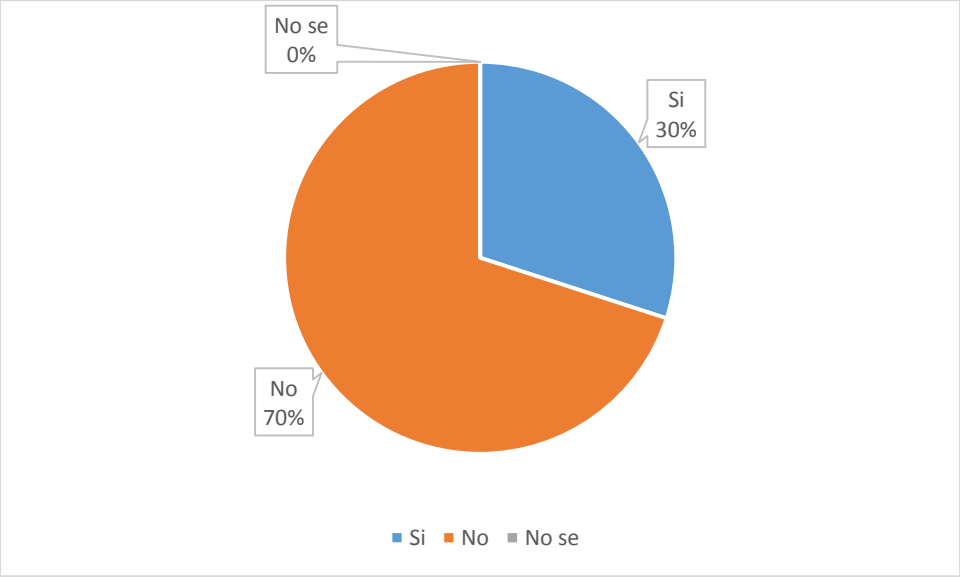

Gráfico 56. Pregunta No. 56

Análisis 56: Los sistemas de información del 70% de las empresas encuestadas no cuentan con ningún tipo de registro y monitoreo de pistas de auditorías, mientras que el 30% restante mencionan poseer registros de actividades realizadas en sistemas, asegurándose de ésta forma tener control sobre los eventos realizados durante la operación de dichos sistemas.

Recomendación 56: Debería implementarse controles para el registro y monitoreo de información transaccional consideradas críticas para la organización.

Pregunta No. 57

¿Los servidores se encuentran sincronizados con una única fuente de tiempo de referencia?

Objetivo 57:

Determinar si se ha implementado controles para mantener sincronizados los relojes de todos los sistemas de procesamiento de información y en relación con una fuente de sincronización única de referencia.

Alternativa	Frecuencia	Porcentaje
Si	4	40%
No	2	20%
No se	4	40%
Total	10	100%

Tabla 62. Pregunta No. 57

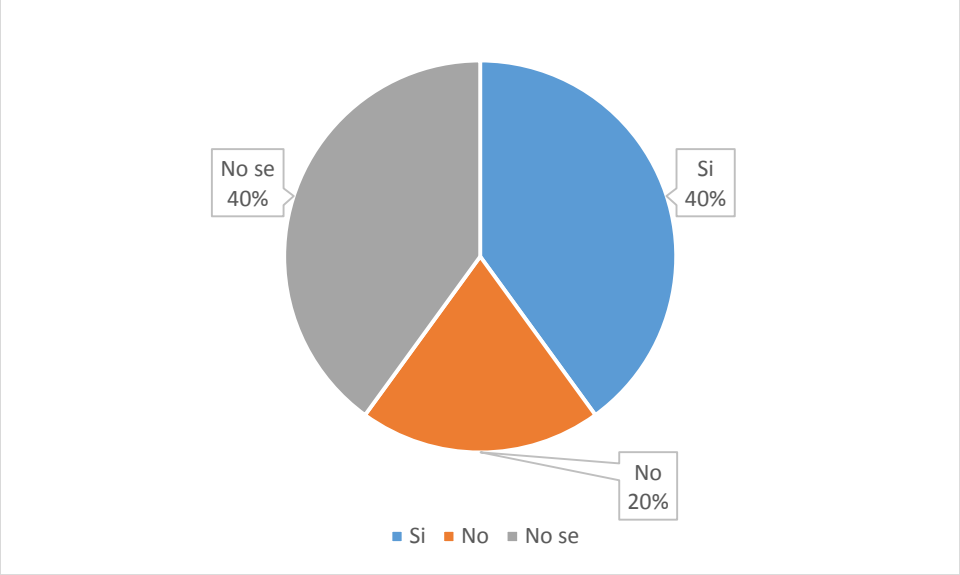

Gráfico 57. Pregunta No. 57

Análisis 57: Al menos el 20% manifiestan que los servidores no se encuentran sincronizados con única fuente de tiempo, existe un 40% que desconoce si aplican ésta medida, mientras que el resto afirman que han implementado dicha medida. La falta de implementación de ésta medida afecta la integridad de la información y aún posible análisis de la misma.

Recomendación 57: La organización debería establecer una única fuente de referencia de tiempo para todos los sistemas de procesamiento de información.

Control de software operacional

Objetivo: Asegurar la integridad de los sistemas operacionales

Pregunta No. 58

¿Existe un control para la instalación de software no autorizado en los sistemas operacionales?

Objetivo 58:

Determinar si la organización implementa procedimientos para controlar la instalación de software en sistemas operacionales.

Alternativa	Frecuencia	Porcentaje
Si	1	10%
No	9	90%
No se	0	0%
Total	**10**	**100%**

Tabla 63. Pregunta No. 58

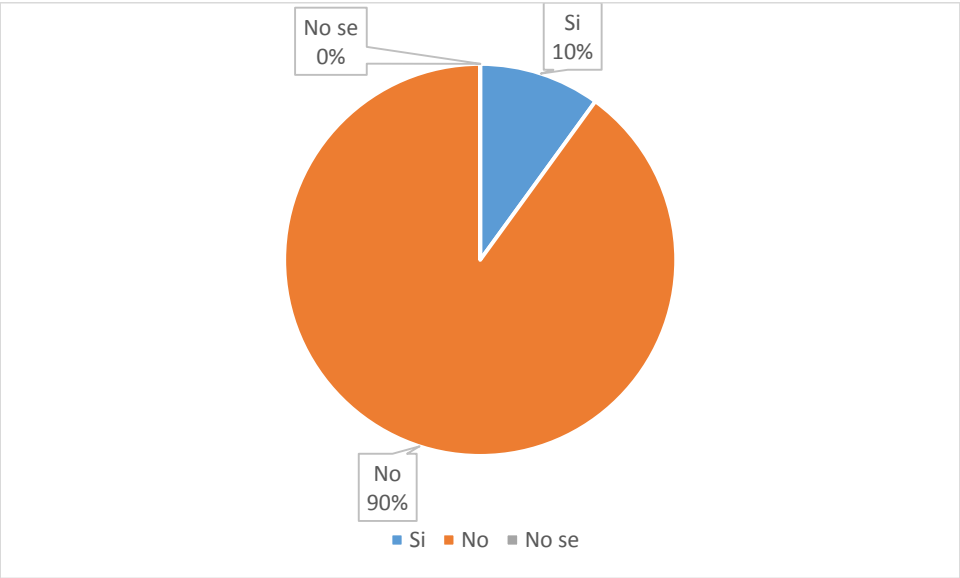

Gráfico 58. Pregunta No. 58

Análisis 58: Es evidente que no existen controles que garanticen la instalación de software no autorizado en los sistemas operacionales, ya que, el 90% de las empresas encuestadas manifestaron no poseer ninguna medida para controlar la instalación de software en dichos sistemas.

Recomendación 58: La organización debe implementar medidas que regulen la instalación de software no autorizado en sistemas operacionales.

Gestión de la vulnerabilidad técnica

Objetivo: Prevenir la explotación de vulnerabilidades técnicas

Pregunta No. 59

¿Existe un procedimiento para la actualización e instalación de parches de seguridad en los sistemas de información?

Alternativa	Frecuencia	Porcentaje
Si	2	20%
No	8	80%
No se	0	0%
Total	**10**	**100%**

Tabla 64. Pregunta No. 59

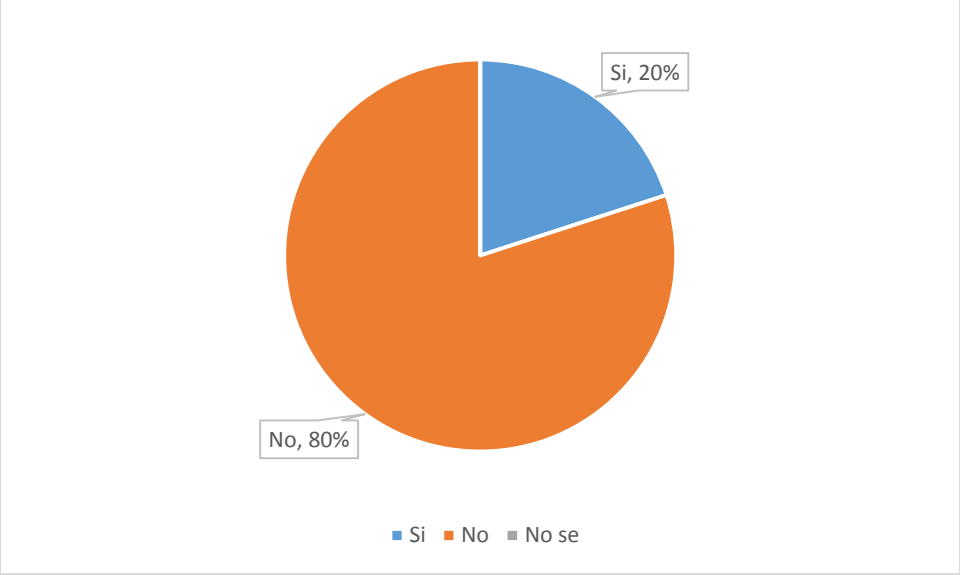

Gráfico 59. Pregunta No. 59

Objetivo 59:

Conocer si la organización ha implementado procedimientos para controlar el proceso de actualización e instalación de parches de seguridad de los sistemas de información.

Análisis 59: Con base en los resultados obtenidos es posible determinar que las empresas encuestadas no cuentan con ningún procedimiento para la instalación de parches de seguridad en sus sistemas de información. Esta situación genera una vulnerabilidad que afecta la confidencialidad, integridad y disponibilidad de la información.

Recomendación 59: La dirección debe asegurar que se implementan procedimientos para la instalación de parches de seguridad para los sistemas de información e infraestructura tecnológica.

Pregunta No. 60

¿Existe un control para la instalación de software no autorizado en los equipos asignados a empleados?

Objetivo 60: Determinar la existencia de controles que regulen la instalación de software a los equipos asignados a los empleados.

Alternativa	Frecuencia	Porcentaje
Si	0	0%
No	10	100%
No se	0	0%
Total	**10**	**100%**

Tabla 65. Pregunta No. 60

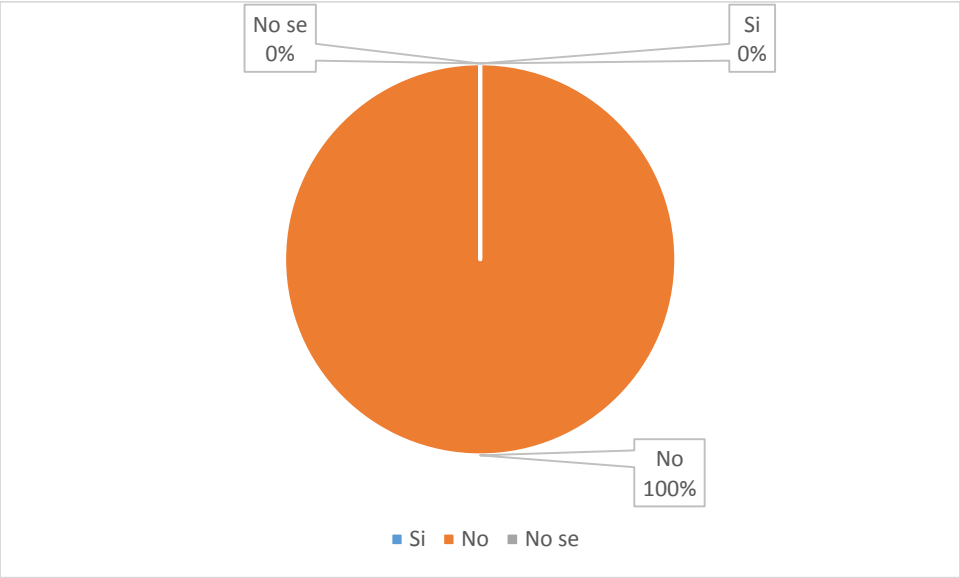

Gráfico 60. Pregunta No. 60

Análisis 60: Los resultados reflejan que el 100% de las empresas encuestadas no implementan medidas para controlar la instalación de software no autorizado en los equipos asignados a empleados. Esta situación podría comprometer la seguridad de cada uno de los equipos.

Recomendación 60: Debe implementarse medidas que limiten la instalación de software no autorizado en equipos asignados a los empleados. Adicionalmente la organización de definir un inventario de software permitido.

Parte X: Seguridad en las comunicaciones. Transferencia de información

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa

Pregunta No. 61

¿Existen mecanismos de aseguramiento para la transferencia de información por medios físicos y/o digitales?

Objetivo 61: Identificar si la organización implementa medidas de control para asegurar la información que se transfiere a través de medios físicos y/o digitales.

Alternativa	Frecuencia	Porcentaje
Si	0	0%
No	10	100%
No se	0	0%
Total	**10**	**100%**

Tabla 66. Pregunta No. 61

Gráfico 61. Pregunta No. 61

Análisis 61: La totalidad de las empresas manifiestan no poseer medidas que aseguren que la información transferida por medios físicos y/o digitales no pueda ser objetivo de robo o modificación que afecten su integridad y/o confidencialidad.

Recomendación 61: La organización debería adoptar medidas para controlar que la transferencia de información por medios físicos y/o digitales se realice de forma segura.

Pregunta No. 62

¿Existen acuerdos de seguridad para la transferencia y protección de la información entre la organización y entidades externas?

Objetivo 62: Determinar si la organización implementa medidas de seguridad para resguardar el acceso no autorizado a la información transferida entre la empresa y entidades externas.

Alternativa	Frecuencia	Porcentaje
Si	1	10%
No	9	90%
No se	0	0%
Total	**10**	**100%**

Tabla 67. Pregunta No. 62

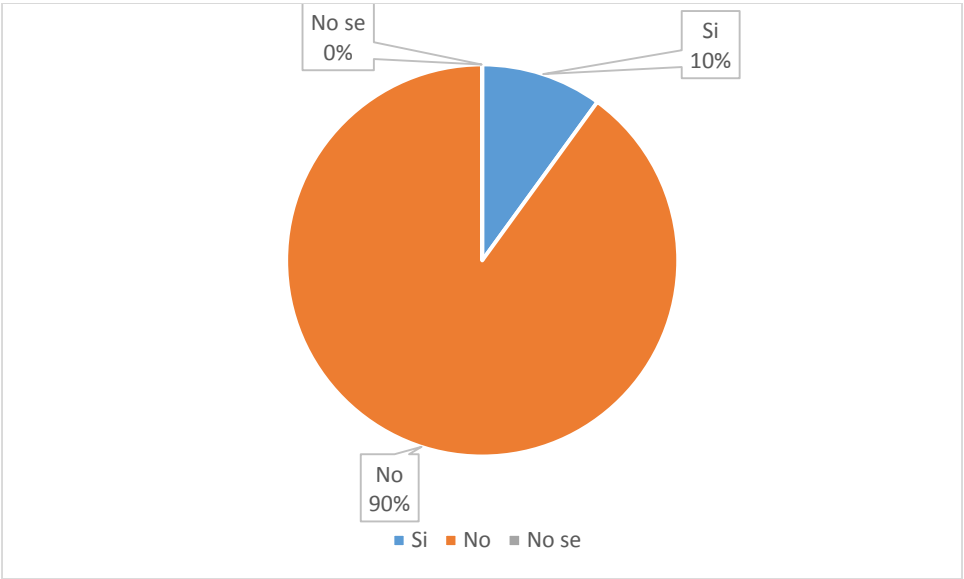

Gráfico 62. Pregunta No. 62

Análisis 62: Un alto porcentaje de las empresas encuestadas manifestaron que no cuentan con medidas para proteger la transferencia de información con otras entidades. Se debe

aprovechar el porcentaje mayor negativo para hacer ver a las empresas la necesidad de implementar controles para resguardar la confidencialidad e integridad de la información que es transferida a otras organizaciones.

Recomendación 62: La organización debería establecer controles para proteger la información transferida a otras entidades.

Parte XI: Adquisición, desarrollo y mantenimiento de sistemas. Requisitos de seguridad de los sistemas de información

Objetivo: Asegurar que la seguridad de la información es una parte integral de los sistemas de información a través de todo su ciclo de vida. Esto también incluye los requerimientos para sistemas de información que proveen servicios sobre redes públicas.

Pregunta No. 63

¿Se identifican y documentan los requisitos de seguridad de los sistemas de información antes de su desarrollo y/o implantación?

Objetivo 63: Identificar si los requerimientos de seguridad de la información son incluidos en el desarrollo de nuevos sistemas de información o mejoras a sistemas existentes.

Alternativa	Frecuencia	Porcentaje
Si	2	20%
No	8	80%
No se	0	0%
Total	**10**	**100%**

Tabla 68. Pregunta No. 63

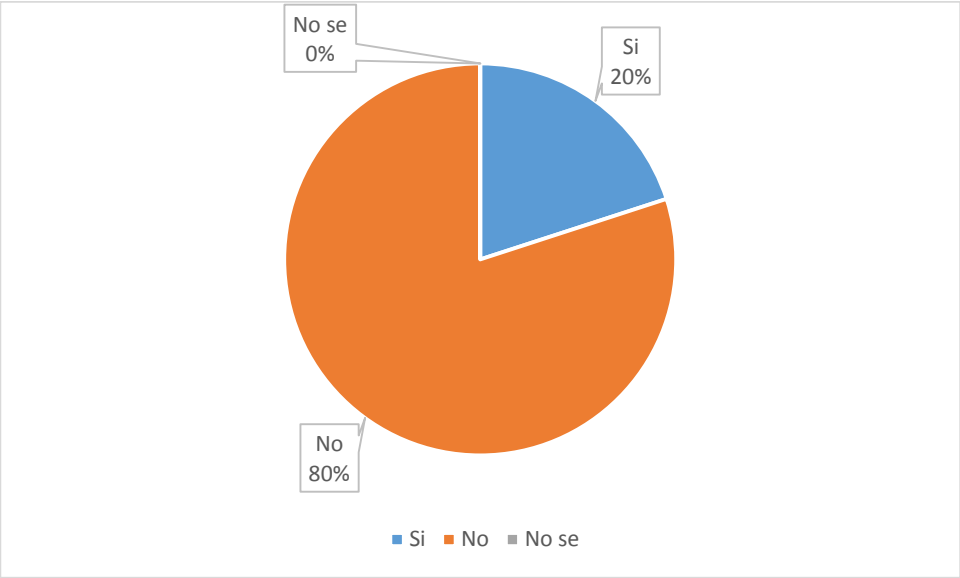

Gráfico 63. Pregunta No. 63

Análisis 63: Con base a los resultados es posible observar que el 80% de las empresas no toman en cuenta requisitos de seguridad para el desarrollo y/o implantación de nuevos sistemas. Como consecuencia de la ausencia de éste control podría generase vulnerabilidades que afecten la confidencialidad, integridad y disponibilidad de la información.

Recomendación 63: Para las organizaciones que poseen equipos de desarrollo interno o para aquellas que implementan soluciones externas, debe asegurar que durante el ciclo de vida de los sistemas de información la seguridad sea parte integral de éstos.

Pregunta No. 64

¿Se implementan controles para proteger la información transaccional de los servicios de aplicación que pasan a través de redes públicas y/o privadas?

Objetivo 64: Identificar la existencia de controles que protejan la transferencia de información a través de redes públicas y/o privadas.

Alternativa	Frecuencia	Porcentaje
Si	1	10%
No	9	90%
No se	0	0%
Total	**10**	**100%**

Tabla 69. Pregunta No. 64

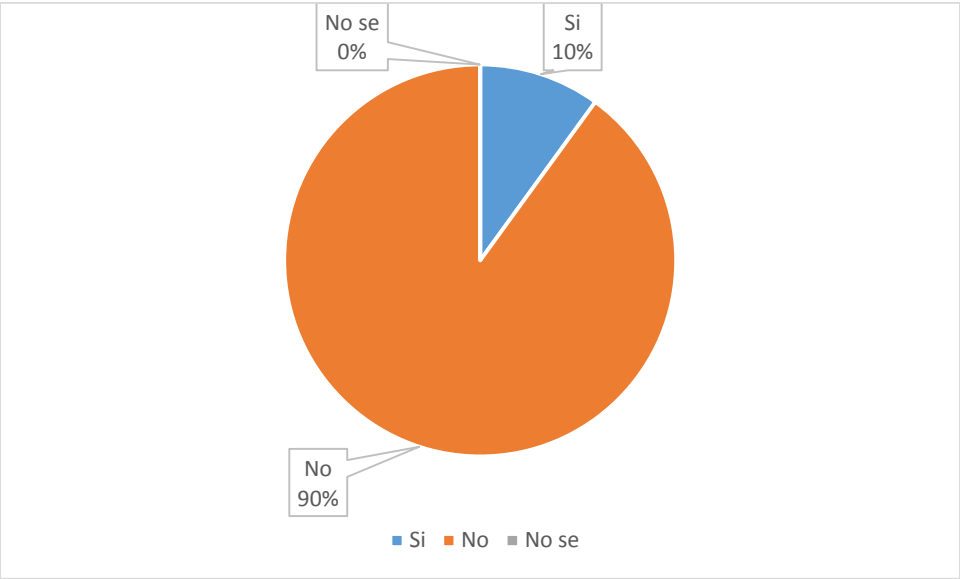

Gráfico 64. Pregunta No. 64

Análisis 64: Es claro que la mayor parte de las empresas no implementan ningún tipo de control para la transferencia de información de forma segura a través de redes públicas y/o privadas comprometiendo la confidencialidad e integridad de la misma.

Recomendación 64: Las organizaciones deben asegurar la implementación de medidas básicas para proteger la información que se transfiere a través de redes públicas y/o privadas.

Seguridad en los procesos de desarrollo y soporte

Objetivo: Asegurar que la seguridad de la información es diseñada e implementada dentro del ciclo de visa de desarrollo de sistemas de información

Pregunta No. 65

¿Se establecen y aplican reglas para el desarrollo de software y sistemas seguros dentro de la organización?

Objetivo 65: Conocer si las organizaciones establecen o aplican reglas para el desarrollo de software dentro de la organización.

Alternativa	Frecuencia	Porcentaje
Si	1	10%
No	9	90%
No se	0	0%

Total	**10**	**100%**

Tabla 70. Pregunta No. 65

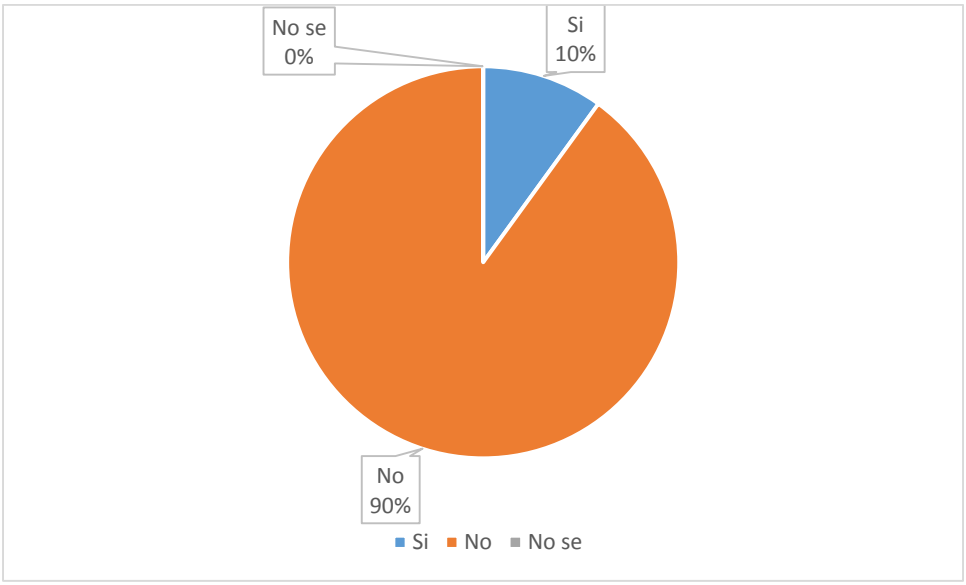

Gráfico 65. Pregunta No. 65

Análisis 65: Es evidente que las empresas encuestadas no implementan ningún tipo de lineamientos para el desarrollo seguro de software dentro de la organización. Tal como se mencionó en el análisis de la pregunta 63, la ausencia de éste tipo de controles podría genera vulnerabilidades que afecten la confidencialidad, integridad y disponibilidad de la información.

Recomendación 65: En el caso que la organización decida ejecutar un proyecto de desarrollo de software, deberá incorporar la seguridad de la información en todas las fases de su ejecución.

Pregunta No. 66

¿Existe un procedimiento para el control de cambios a los sistemas dentro del ciclo de vida de desarrollo?

Objetivo 66: Conocer si las organizaciones implementan medidas para controlar los cambios dentro del ciclo de vida de desarrollo de sistemas existentes.

Alternativa	Frecuencia	Porcentaje
Si	1	10%
No	9	90%
No se	0	0%

Total	**10**	**100%**

Tabla 71. Pregunta No. 66

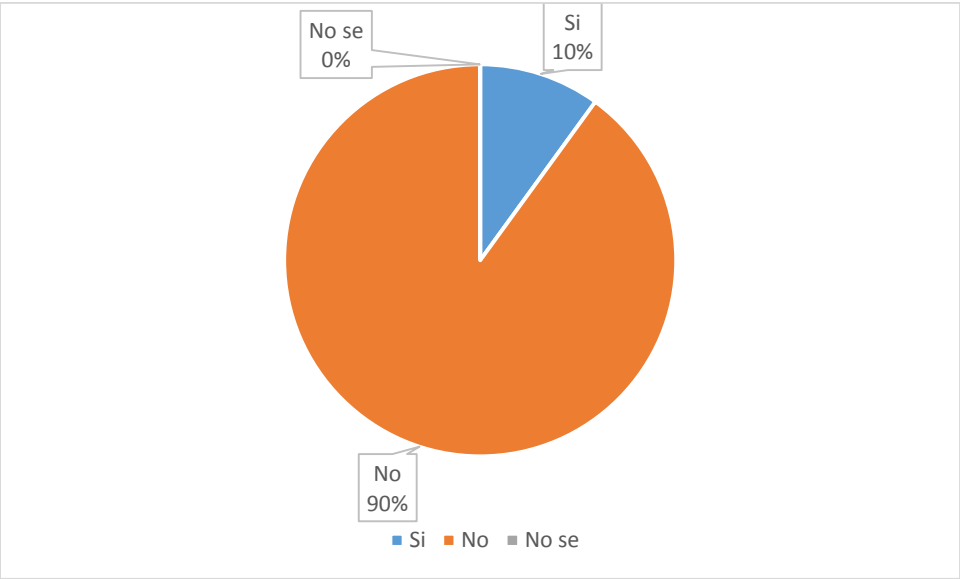

Gráfico 66. Pregunta No. 66

Análisis 66: El 90% de las empresas encuestadas manifestaron que no poseen medidas para gestionar el control de cambios de un sistema dentro del ciclo de vida de su desarrollo. La falta de éstas medidas podría generar una afectación en la disponibilidad e integridad de los sistemas.

Recomendación 66: En el caso que la organización contemple el desarrollo de sistemas de información deben incorporar la seguridad de la información desde la concepción hasta la desaparición de un sistema.

Pregunta No. 67

Ante un cambio de plataforma operativa, ¿se realizan las pruebas necesarias para garantizar la operación de los sistemas de información?

Objetivo 67: Conocer si las organizaciones realizan pruebas necesarias de los sistemas de información para garantiza su operatividad.

Alternativa	Frecuencia	Porcentaje
Si	6	60%
No	4	40%
No se	0	0%
Total	**10**	**100%**

Tabla 72. Pregunta No. 67

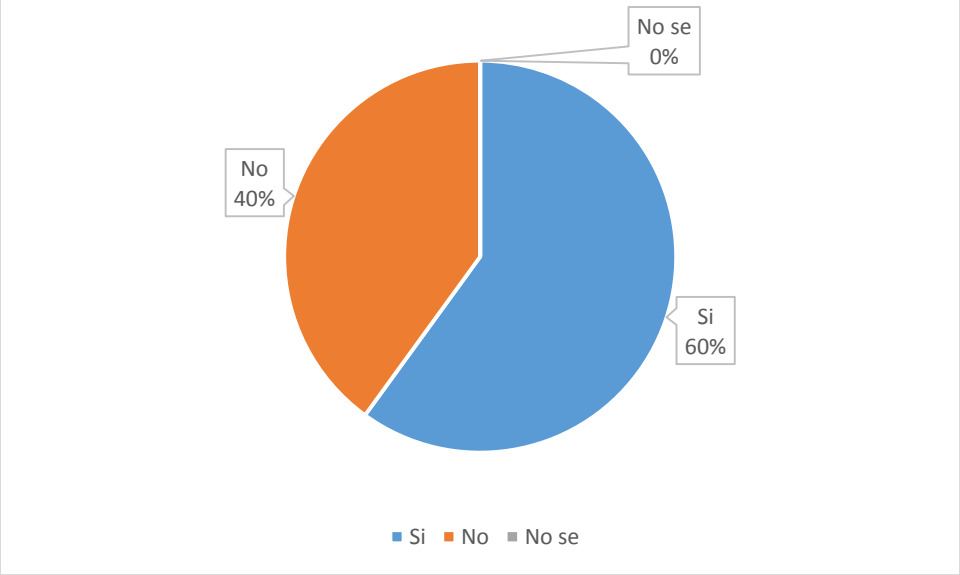

Gráfico 67. Pregunta No. 67

toma en cuenta medidas de seguridad ante cambios de plataforma operativa

Análisis 67: Existe casi una paridad sobre los resultados obtenidos de las empresas que contemplan la realización de pruebas necesarias para garantizar la operación de sistemas de información.

Recomendación 67: Previo a un cambio de plataforma tecnológica, la organización debe realizar las pruebas necesarias para garantizar la operatividad de los sistemas de información.

Pregunta No. 68

¿La organización establece y protege los entornos de desarrollo seguro?

Objetivo 68:

Identificar si la organización establece políticas o lineamientos para proteger los ambientes de desarrollo seguro.

Alternativa	Frecuencia	Porcentaje
Si	0	0%
No	9	90%
No se	1	10%
Total	**10**	**100%**

Tabla 73. Pregunta No. 68

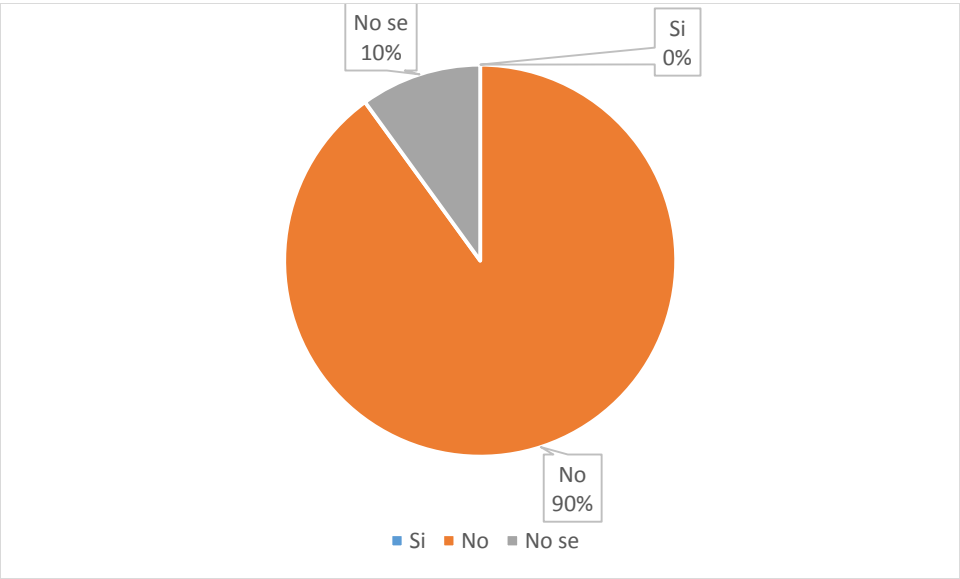

Gráfico 68. Pregunta No. 68

Análisis 68: En éste punto se ha obtenido un resultado alarmante ya que el 100% de las empresas encuestadas manifiestan no poseer o desconocer la existencia de lineamientos o políticas que protejan los entornos de desarrollo seguro. La falta de éste tipo de controles podría afectar la integridad de los sistemas de información.

Recomendación 68: En los casos en que las empresas desarrollen interna o externamente sus sistemas de información, deben considerar la definición de reglas, políticas o lineamientos que indiquen la forma de proteger los ambientes de desarrollo de sistemas de información.

Pregunta No. 69

En los casos en que se subcontrate el desarrollo de software, ¿existe una supervisión y monitoreo de las actividades realizadas durante el desarrollo de los sistemas?

Objetivo 69:

Identificar si existe una supervisión y monitoreo de las actividades realizadas durante el desarrollo subcontratado de sistemas.

Alternativa	Frecuencia	Porcentaje
Si	5	50%
No	4	40%

No se	1	10%
Total	**10**	**100%**

Tabla 74. Pregunta No. 69

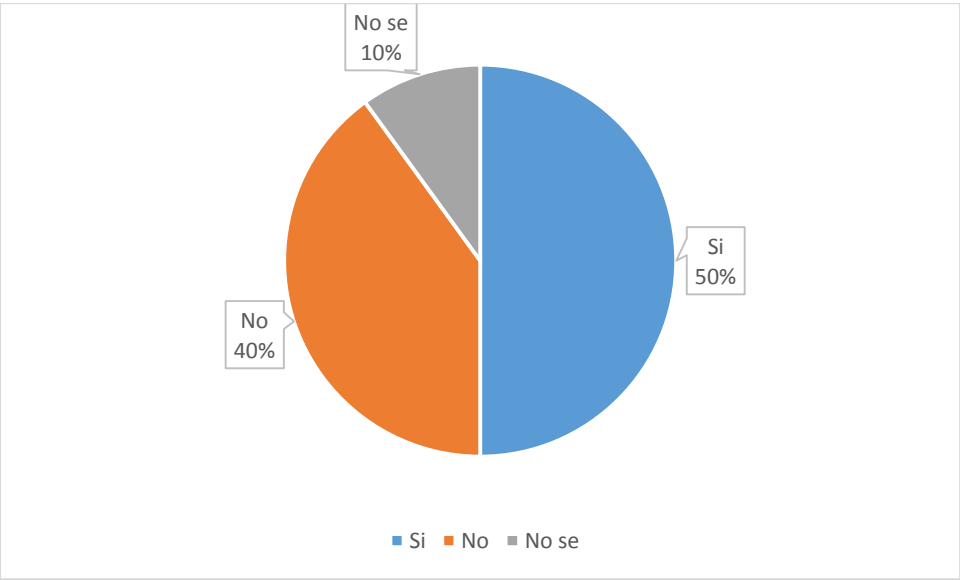

Gráfico 69. Pregunta No. 69

Análisis 69: Al menos el 50% de las empresas encuestadas manifiestan que realizan algún tipo de supervisión o monitoreo de las actividades realizadas durante el desarrollo de sistemas, el 50% restante respondió desconocer o que no se realizan.

Recomendación 69: Debe existir una supervisión de la organización para los casos en que se subcontrate el desarrollo de software.

Pregunta No. 70

¿La organización realiza pruebas de seguridad de los sistemas previo a ponerlos en la fase operativa?

Objetivo 70: Identificar si la organización ha definido procedimientos para realizar pruebas de funcionalidad de los sistemas previo a ponerlos en la fase operativa.

Alternativa	Frecuencia	Porcentaje
Si	4	40%
No	6	60%
No se	0	0%
Total	**10**	**100%**

Tabla 75. Pregunta No. 70

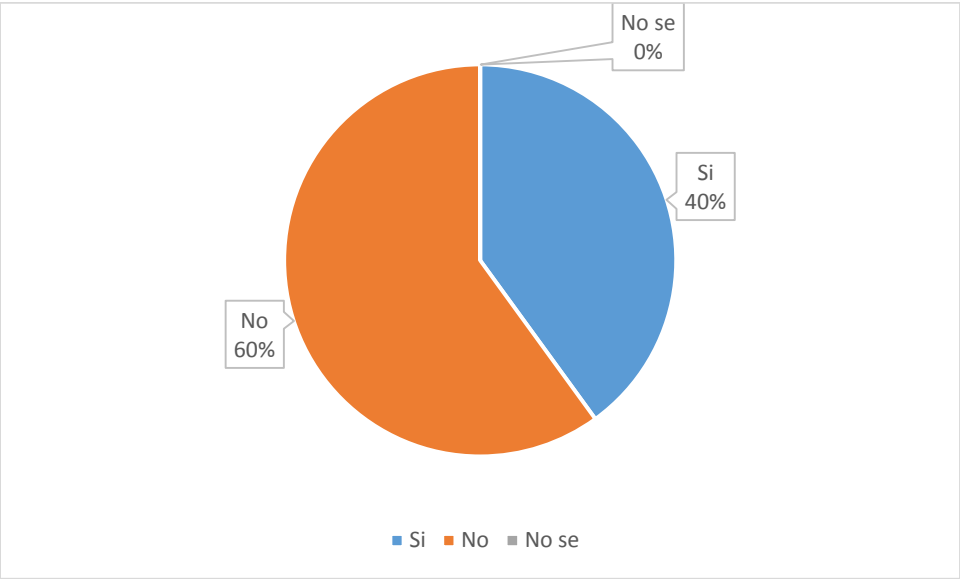

Gráfico 70. Pregunta No. 70

Análisis 70: Conforme a los datos obtenidos, es posible identificar que un 40% de las empresas encuestadas posee algún tipo de procedimientos para realizar pruebas de seguridad de los sistemas previo a iniciar la fase operativa. Sin embargo, es preocupante que el 60% de las empresas no contemplen la realización de éste tipo de pruebas.

Recomendación 70: Se deben establecer baterías de pruebas básicas para garantizar la seguridad de los sistemas en la fase operativa.

Pregunta No. 71

¿Se establecen programas de pruebas de aceptación de los nuevos sistemas de información, actualizaciones y nuevas versiones?

Objetivo 71: Identificar si la organización contempla la realización de pruebas de aceptación dentro del ciclo de vida de sistemas de información.

Alternativa	Frecuencia	Porcentaje
Si	6	60%
No	4	40%
No se	0	0%
Total	**10**	**100%**

Tabla 76. Pregunta No. 71

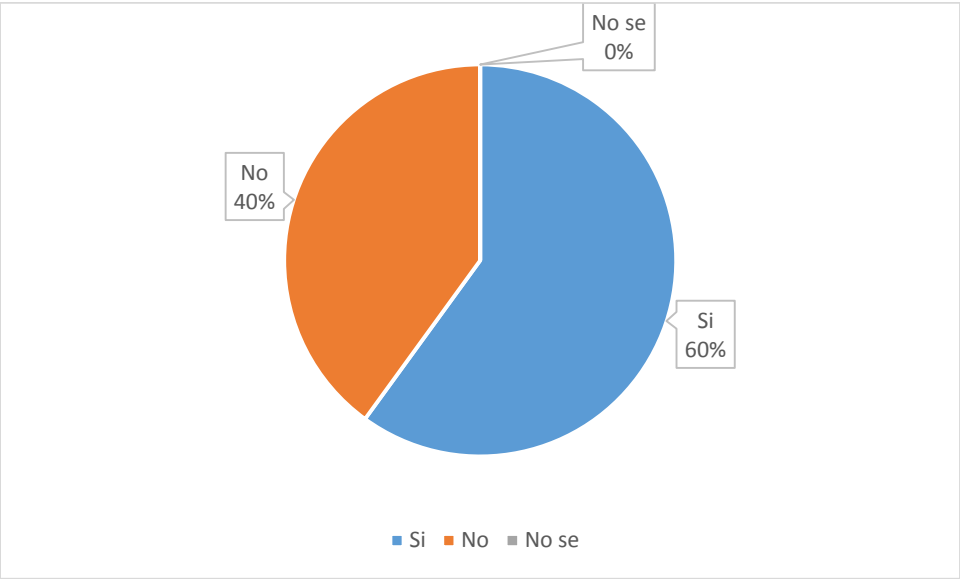

Gráfico 71. Pregunta No. 71

Análisis 71: Al menos el 60% de las empresas realiza algún tipo de pruebas para asegurar la aceptación de los nuevos desarrollo o cambios de los sistemas de información.

Recomendación 71: Las empresas deben establecer baterías de pruebas básicas para garantizar la aceptación por parte de los usuarios de los nuevos sistemas, actualizaciones o nuevas versiones.

Datos de prueba

Objetivo: Asegurar la protección de los datos usados para pruebas

Pregunta No. 72

¿Los datos utilizados para pruebas son protegidos y resguardados adecuadamente?

Objetivo 72: Conocer si los datos utilizados para las pruebas de los sistemas de información son cuidadosamente seleccionados, protegidos y resguardados.

Alternativa	Frecuencia	Porcentaje
Si	1	10%
No	8	80%
No se	1	10%
Total	**10**	**100%**

Tabla 77. Pregunta No. 72

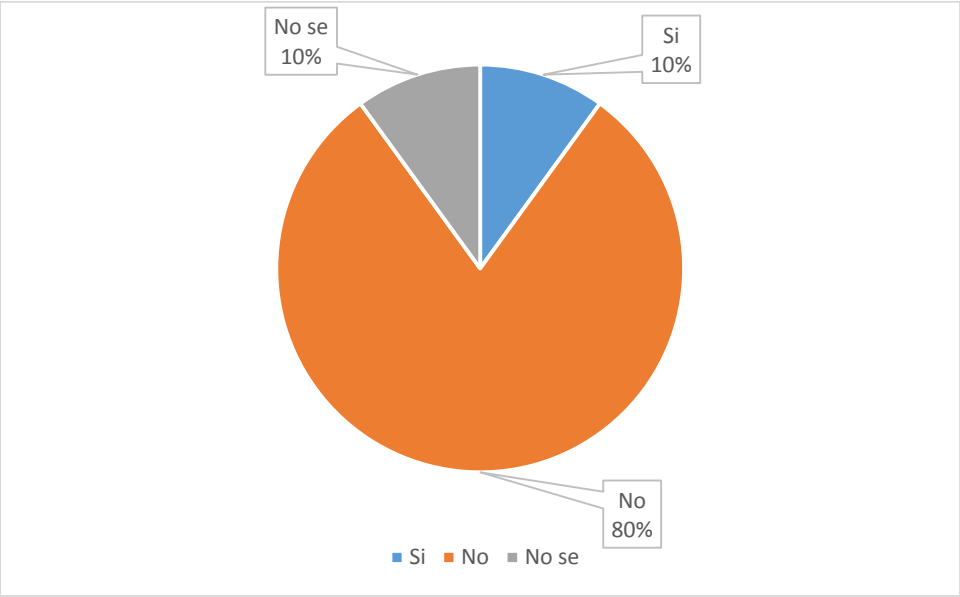

Gráfico 72. Pregunta No. 72

Análisis 72: Se torna preocupante el alto porcentaje de empresas que no implementa medidas para la protección de datos utilizados para pruebas, ya que, la información podría verse comprometida en su confidencialidad.

Recomendación 72: La organización debe implementar las medidas necesarias para garantizar la protección y adecuado resguardo de la información utilizada para pruebas.

Parte XII: Relaciones con proveedores. Seguridad de la información en relaciones con proveedores

Objetivo: Asegurar la protección de los activos de la organización que son accesibles a proveedores

Pregunta No. 73

¿Se cuenta con acuerdos de confidencialidad de la información con los proveedores?

Objetivo 73: Conocer la existencia de políticas de seguridad de la información para la relación con los proveedores.

Alternativa	Frecuencia	Porcentaje
Si	4	40%
No	6	60%
No se	0	0%
Total	**10**	**100%**

Tabla 78. Pregunta No. 73

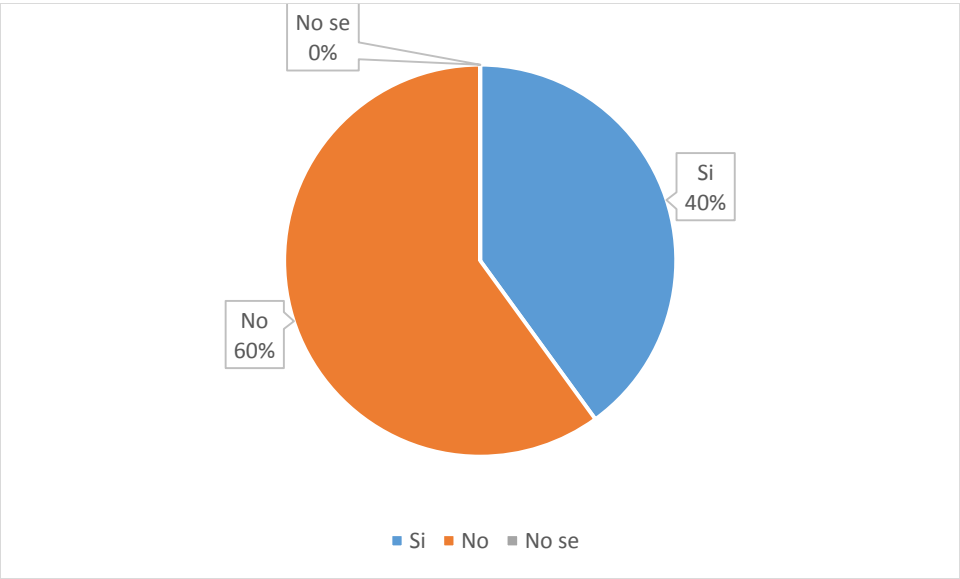

Gráfico 73. Pregunta No. 73

Análisis 73: Con base en los resultados obtenidos es posible afirmar que existe casi una paridad en cuanto a la existencia de acuerdos o políticas de confidencialidad de la información para la relación con los proveedores.

Recomendación 73: Las organizaciones deben establecer acuerdos de la confidencialidad en los contratos de adquisición de servicios con los proveedores.

Gestión de servicio de entrega del proveedor

Objetivos: Mantener un nivel acordado de seguridad de la información y el servicio de entrega alineados con los acuerdos del proveedor

Pregunta No. 74

¿Se realizan monitoreos, revisiones y auditorias periódicas a los servicios que los proveedores entregan?

Objetivo 74: Conocer si las organizaciones contemplan la realización de revisiones y auditorías periódicas del nivel de servicio que los proveedores entregan.

Alternativa	Frecuencia	Porcentaje
Si	1	10%
No	9	90%
No se	0	0%

Total	**10**	**100%**

Tabla 79. Pregunta No. 74

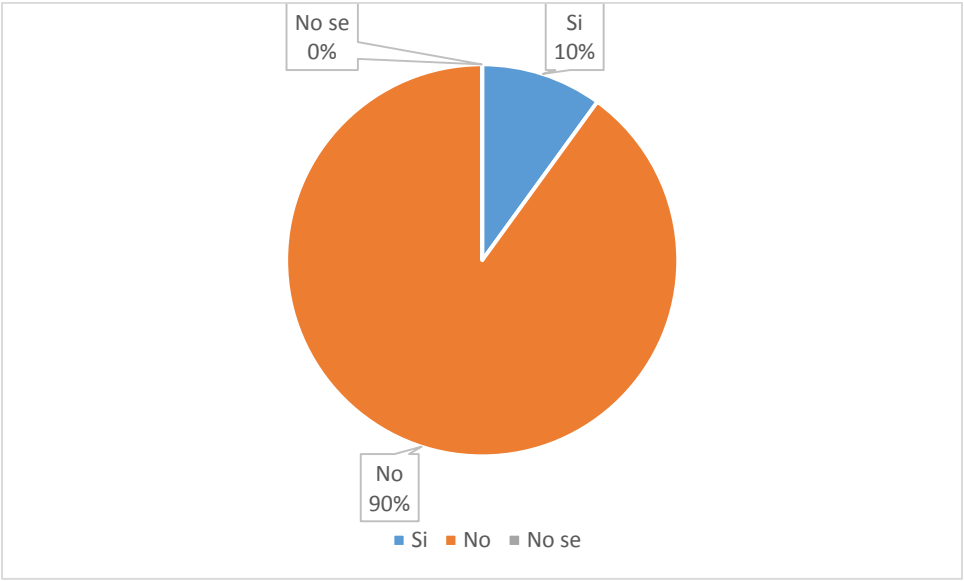

Gráfico 74. Pregunta No. 74

Análisis 74: De acuerdo a los datos obtenidos, un alto porcentaje de las empresas encuestadas manifiestan que no se realizan revisiones o auditorías a los servicios entregados por los proveedores, esta situación afecta la confidencialidad y disponibilidad de la información que sea compartida.

Recomendación 74: La organización debe implementar revisiones y auditorías a las empresas que le prestan servicios.

Parte XIII: Gestión de incidentes de seguridad de la información

Gestión de incidentes de seguridad de la información y mejoras

Objetivo: Asegurar un enfoque consistente y efectivo para la gestión de incidentes de seguridad de la información, incluyendo la comunicación en los eventos y debilidades de seguridad.

Pregunta No. 75

¿Existe un procedimiento para la notificación de eventos de seguridad y vulnerabilidades identificadas conocidas por toda la institución que garantice una respuesta rápida y efectiva?

Objetivo 75: Determinar la existencia de procedimientos documentados para que los eventos de seguridad de la información sean comunicados a través de los canales de administración adecuados tan pronto como sea posible.

Alternativa	Frecuencia	Porcentaje
Si	0	0%
No	10	100%
No se	0	0%
Total	**10**	**100%**

Tabla 80. Pregunta No. 75

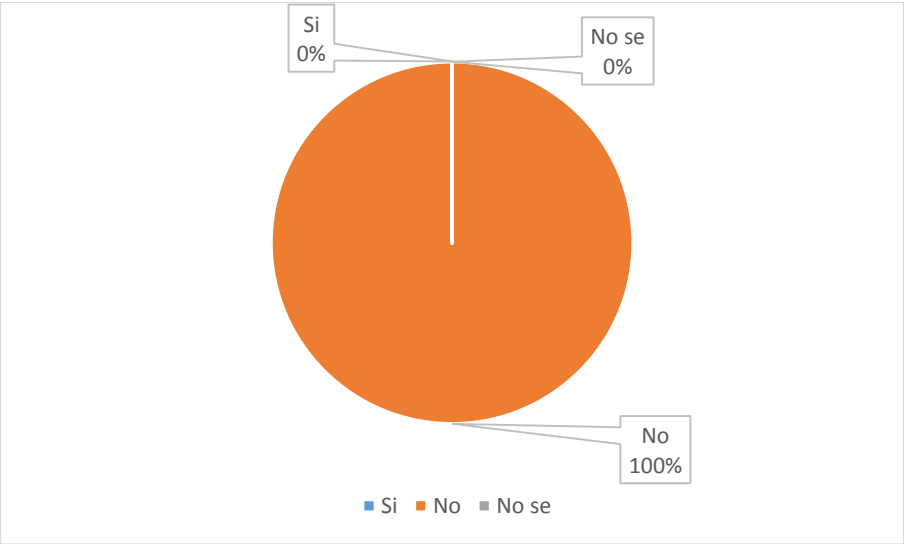

Gráfico 75. Pregunta No. 75

Análisis 75: Es claro que en empresas encuestadas no existe un procedimiento para la notificación de eventos de seguridad y vulnerabilidades identificadas conocidas por toda la institución que garantice una respuesta rápida y efectiva.

Recomendación 75: Debería implementarse un mecanismo para la notificación de eventos e incidentes de seguridad.

Pregunta No. 76

¿Existen procedimientos documentados para dar respuesta a los incidentes de seguridad?

Objetivo 76: Identificar si la organización cuenta con procedimientos para la designación de responsabilidades, atención y notificación de incidentes de seguridad de la información

Alternativa	Frecuencia	Porcentaje
Si	0	0%
No	10	100%
No se	0	0%
Total	**10**	**100%**

Tabla 81. Pregunta No. 76

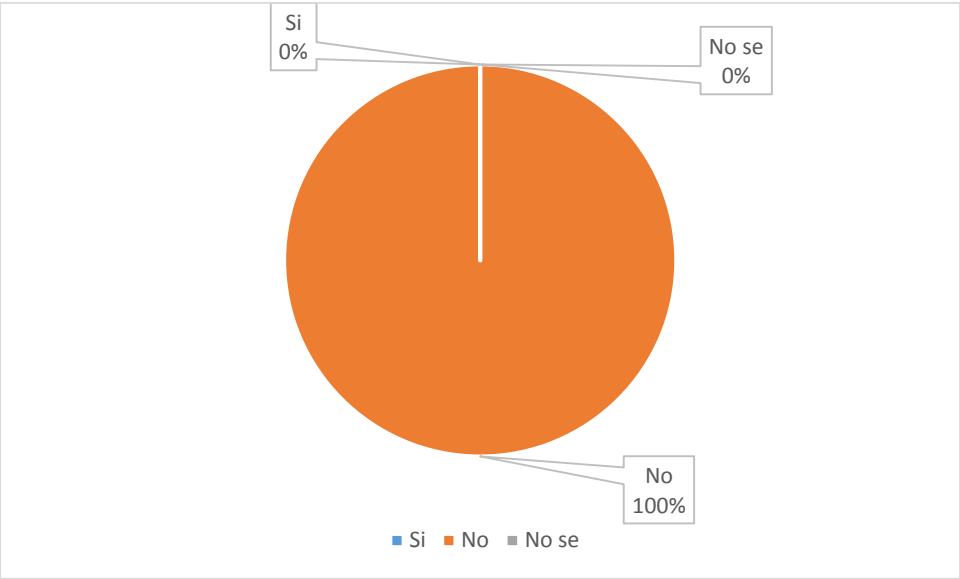

Gráfico 76. Pregunta No. 76

Análisis 76: Con base a los resultados obtenidos es posible afirmar que las PYMES encuestadas no consideran relevante la documentación de seguridad relacionada con los procedimientos de respuesta a incidentes de seguridad.

Recomendación 76: La organización debería establecer procedimientos de seguridad para dar respuesta a incidentes de seguridad.

Pregunta No. 77

¿Los responsables de la gestión de incidentes conocen y aplican los protocolos para la recolección de evidencias?

Objetivo 77: Identificar si existe un conocimiento de parte de los responsables de llevar a cabo la gestión de incidentes para la identificación, recolección, adquisición y preservación de información que pueda ser utilizada como evidencia.

Alternativa	Frecuencia	Porcentaje
Si	0	0%
No	10	100%
No se	0	0%
Total	**10**	**100%**

Tabla 82. Pregunta No. 77

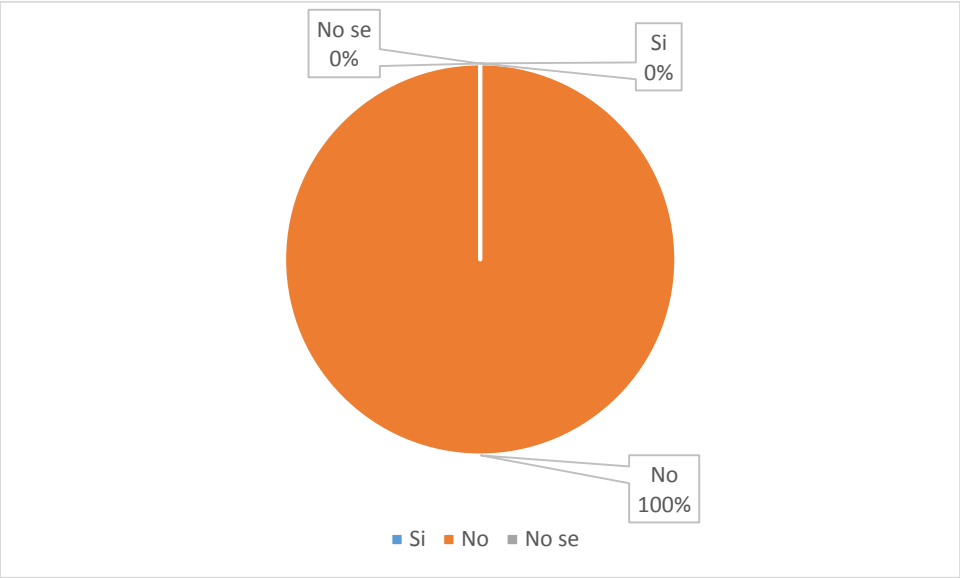

Gráfico 77. Pregunta No. 77

Análisis 77: Las empresas no han definido los responsables para la gestión de incidentes.

Recomendación 77: La organización debería definir responsables de la gestión de incidentes y capacitarles en los protocolos para la recolección de evidencias.

Parte XIV: Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Continuidad de la seguridad de la información

Objetivo: La continuidad de la seguridad de la información debe estar incluida en los sistemas de gestión de la continuidad del negocio de la organización

Pregunta No. 78

¿La organización cuenta con un Plan de Continuidad de Negocio aprobado?

Objetivo 78: Determinar si la organización cuenta con un plan de continuidad del negocio debidamente documentado y aprobado para su implementación.

Alternativa	Frecuencia	Porcentaje
Si	0	0%
No	10	100%
No se	0	0%
Total	**10**	**100%**

Tabla 83. Pregunta No. 78

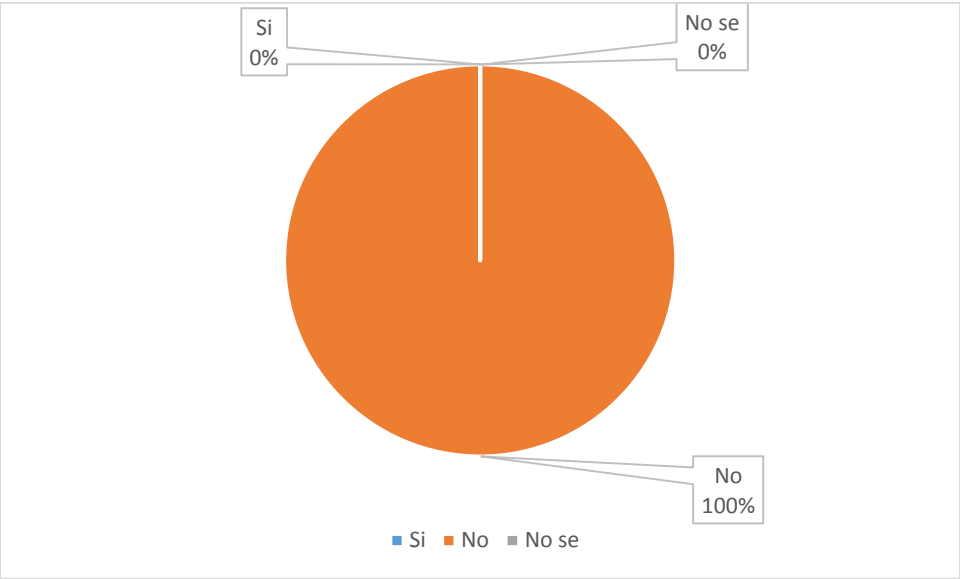

Gráfico 78. Pregunta No. 78

Análisis 78: Las empresas manifestaron que no cuentan con un Plan de Continuidad de Negocio elaborado.

Recomendación 78: La organización debe definir y aprobar un plan de continuidad de negocio basado en los procesos considerados críticos para la organización.

Redundancias

Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de la información

Pregunta No. 79

¿Dispone la organización de sitios alternos a ser utilizados en casos de crisis o desastre?

Objetivo 79: Identificar si la organización cuenta con sitios alternos para garantizar la continuidad de las operaciones ante cualquier crisis o desastre.

Alternativa	Frecuencia	Porcentaje
Si	2	20%
No	8	80%
No se	0	0%
Total	**10**	**100%**

Tabla 84. Pregunta No. 79

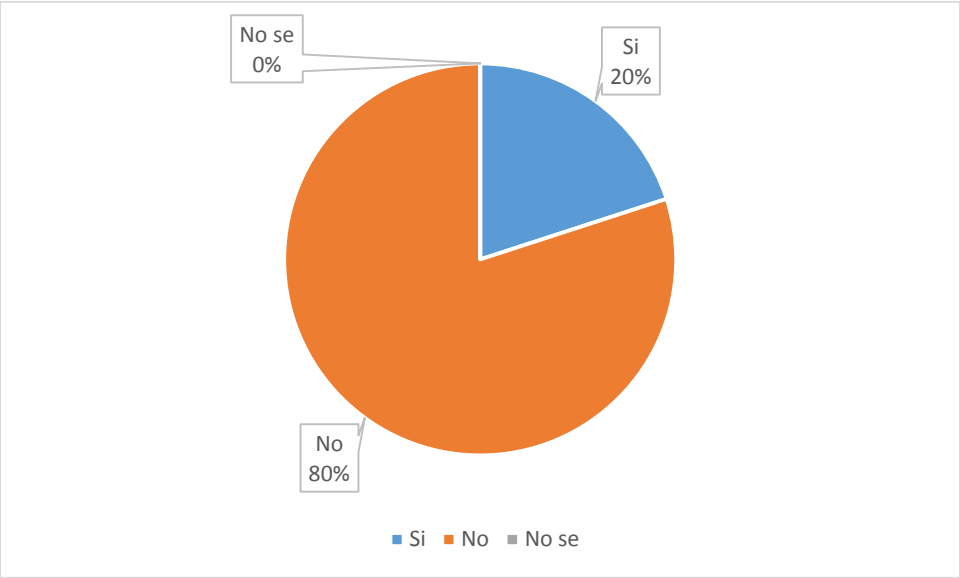

Gráfico 79. Pregunta No. 79

Análisis 79: UN alto porcentaje de empresas no cuenta con un sitio alterno que le permita garantizar la continuidad de las operaciones para los procesos críticos de negocio en caso de crisis o desastre.

Recomendación 79: Se debería considerar poseer al menos un sitio de contingencia ubicado físicamente en una diferente zona geográfica.

Parte XV: Cumplimiento

Cumplimiento con requerimientos legales y contractuales

Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de cualquier requerimiento de seguridad

Pregunta No. 80

¿Se ha identificado, documentado y actualizado los sistemas de información en relación a todos los requerimientos legales, regulaciones y requerimientos contractuales relevantes?

Objetivo 80: Determinar si todos los estatus legales, regulaciones y requerimientos contractuales se encuentran explícitamente identificados y actualizados para cada sistema de información y la organización

Alternativa	Frecuencia	Porcentaje
Si	6	60%
No	4	40%
No se	0	0%
Total	**10**	**100%**

Tabla 85. Pregunta No. 80

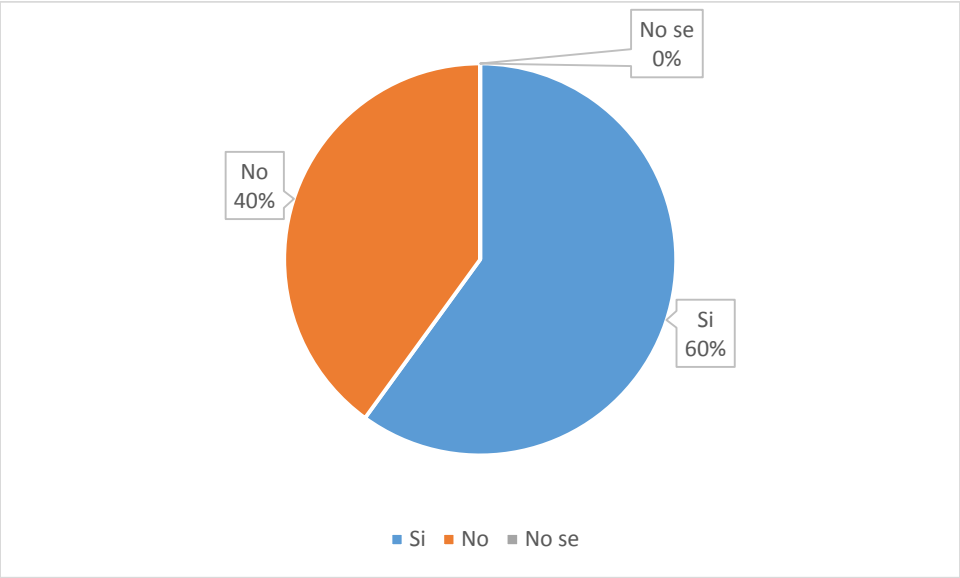

Gráfico 80. Pregunta No. 80

Análisis 80: Es preocupante que los sistemas de información del 40% de las empresas no contemple todos los requerimientos legales y contractuales.

Recomendación 80: La organización debe garantizar que los sistemas de información cumplen con todos los requerimientos legales, regulaciones y requerimiento contractuales.

Pregunta No. 81

¿Cumple la organización con la legislación relacionada a derechos de propiedad intelectual?

Objetivo 81: Determinar si existen procedimientos que cumplan con todos los estatus legales, regulaciones y requerimientos contractuales relacionados con los derechos de propiedad intelectual y uso de producto de software propietario.

Alternativa	Frecuencia	Porcentaje
Si	5	50%
No	2	20%
No se	3	30%
Total	**10**	**100%**

Tabla 86. Pregunta No. 81

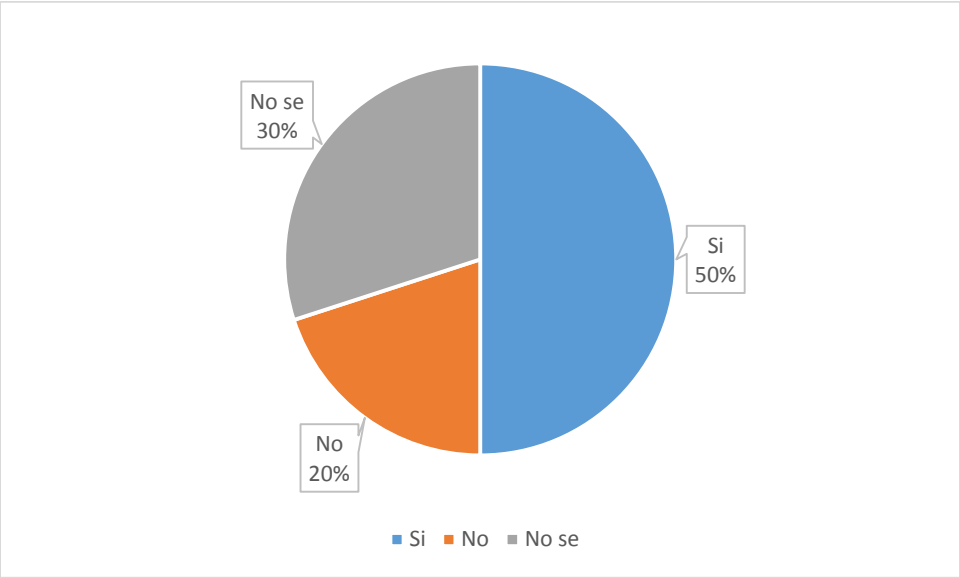

Gráfico 81. Pregunta No. 81

Análisis 81: Es alarmante que el 50% de las empresas manifiestan que desconocen o no dan cumplimiento a los requerimientos establecidos por la legislación relacionada con derechos de propiedad intelectual.

Recomendación 81: Las organizaciones deben garantizar que dan cumplimiento a la legislación relacionada con los derechos de propiedad intelectual.

Pregunta No. 82

¿La organización implementa procedimientos para la protección de registros y para la información identificada como personal?

Objetivo 82: Conocer si existen procedimientos que hagan referencia a la protección de la privacidad de la información catalogada como personal acorde a la legislación y la reglamentación pertinente.

Alternativa	Frecuencia	Porcentaje
Si	2	20%
No	6	60%
No se	2	20%
Total	**10**	**100%**

Tabla 87. Pregunta No. 82

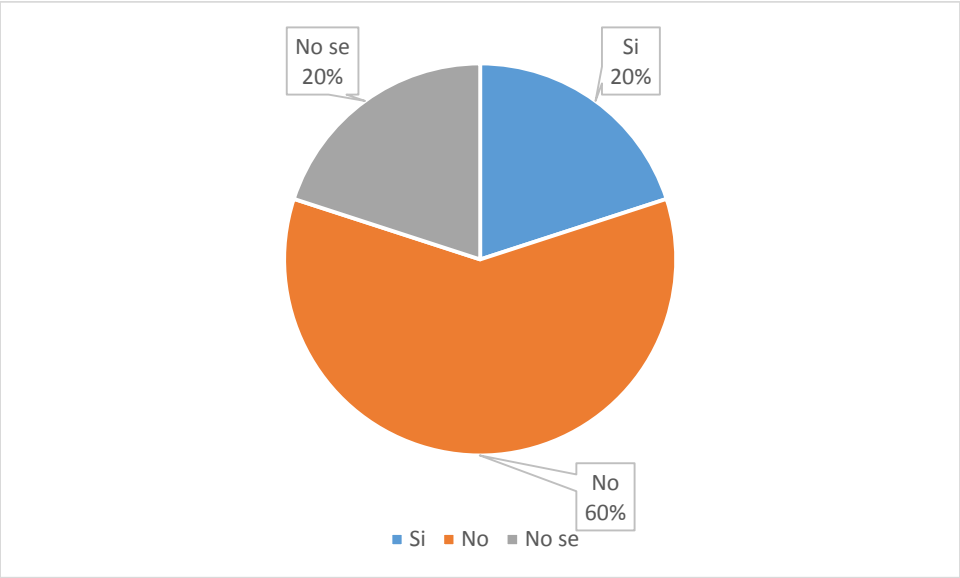

Gráfico 82. Pregunta No. 82

Análisis 82: El resultado obtenido demuestra que solo un 20% de las empresas consideran importante implementar procedimientos para la protección de registros de información personal. El 60% no implementa ningún procedimiento y el 20% desconoce si se implementan.

Recomendación 82: La organización debe implementar políticas o procedimientos para la protección de datos personales.

Pregunta No. 83

¿Utiliza la organización controles criptográficos en cumplimiento con legislaciones, acuerdos o regulaciones pertinentes?

Objetivo 83: Verificar el uso de controles criptográficos en cumplimiento con legislaciones, acuerdos o regulaciones pertinentes.

Alternativa	Frecuencia	Porcentaje
Si	0	0%
No	10	100%
No se	0	0%
Total	**10**	**100%**

Tabla 88. Pregunta No. 83

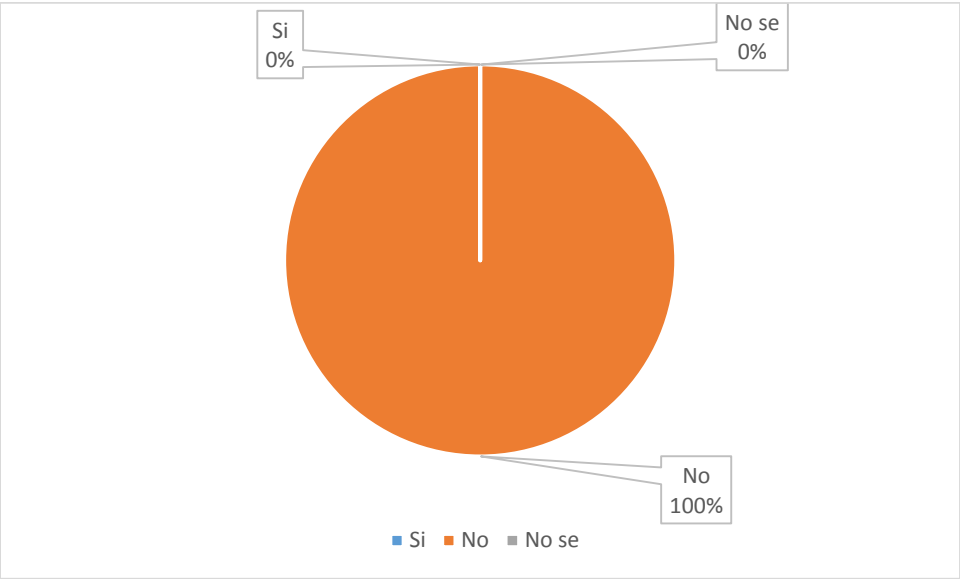

Gráfico 83. Pregunta No. 83

Análisis 83: Es claro que ninguna de las empresas encuestadas considera como medida de seguridad la implementación de controles criptográficos que vayan acorde con el cumplimiento de legislaciones, acuerdos o regulaciones.

Recomendación 83: La organización debería valorar la implementación de controles criptográficos siempre que se requiera en cumplimiento con la legislación o regulaciones pertinentes.

Revisiones de la seguridad de la información

Objetivo: Asegurar que la seguridad de la información se implemente y opere en concordancia con las políticas y procedimientos de la organización.

Pregunta No. 84

¿La organización se apoya en terceros para la auditoría de las políticas, controles, procedimientos de la seguridad de la información?

Objetivo 84: Identificar si existe apoyo de entidades externas para la realización de auditorías para verificar el cumplimiento de políticas, controles y procedimientos de la seguridad de la información.

Alternativa	Frecuencia	Porcentaje
Si	1	10%
No	9	90%
No se	0	0%
Total	**10**	**100%**

Tabla 89. Pregunta No. 84

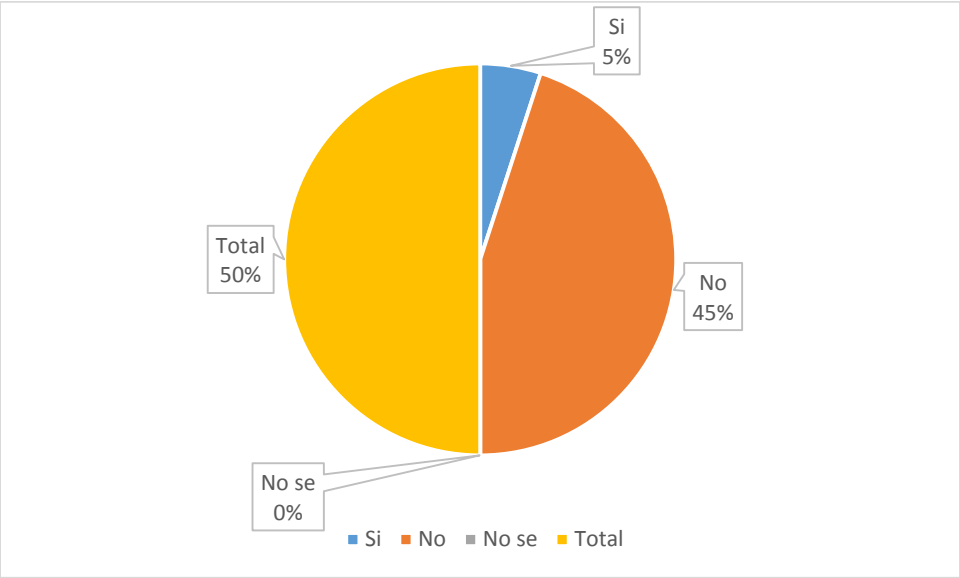

Gráfico 84. Pregunta No. 84

Análisis 84: De acuerdo a lo identificado en la pregunta 7, un alto porcentaje de las empresas manifestó no poseer un documento donde se establezca una política, controles o procedimientos de la seguridad de la información.

Recomendación 84: La organización al poseer una política, controles y procedimientos de la seguridad de la información debe establecer un programa de auditoría de seguridad de seguridad de la información el cual debe ser ejecutado por entidades externas.

Pregunta No. 85

¿Se realizan revisiones periódicas internas del cumplimiento de la política de seguridad, normas, cumplimiento técnico de los sistemas de información y revisión de otros requerimientos de seguridad?

Objetivo 85: Identificar si existe un seguimiento periódico para determinar el cumplimiento que tienen los sistemas de información con respecto a las políticas y normas de seguridad de la información de la organización.

Alternativa	Frecuencia	Porcentaje
Si	2	20%
No	8	80%
No se	0	0%
Total	**10**	**100%**

Tabla 90. Pregunta No. 85

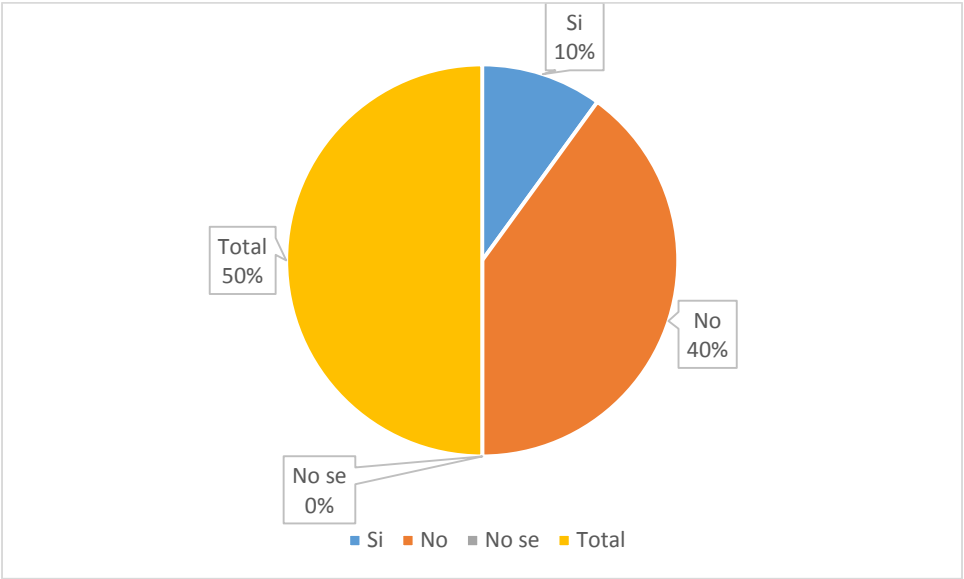

Gráfico 85. Pregunta No. 85

Análisis 85: En concordancia con la respuesta a la pregunta 7, un alto porcentaje de las empresas no cuenta con un documento donde se establezca una política, controles o procedimientos de la seguridad de la información, por tanto, no es posible realizar revisiones periódicas.

Recomendación 85: La organización debe establecer una política, controles y procedimientos de la seguridad de la información y definir períodos de revisión al cumplimiento a lo establecido en dichas políticas.

3. Normalización de la seguridad de la información en El Salvador

3.1. Estándar general para la gestión de la seguridad de la información

3.1.1. Familia de estándares de la 27000

3.1.1.1. ISO/IEC 27000

Publicada el 1 de mayo de 2009, revisada con una segunda edición el 01 de diciembre de 2012 y una tercera edición de 14 de enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de la Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua). Actualmente fuera de vigencia en El Salvador.

3.1.1.2. ISO/IEC 27001

"Publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de la seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados"[5]. Adoptada en El Salvador en fecha 20 de marzo de 2015 bajo el nombre NTS ISO/IEC 27001:2013

3.1.1.3. ISO/IEC 27002

"Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005.

Actualmente, la última edición de 2013 este estándar ha sido actualizada a un total de 14 dominios, 35 objetivos de control y 114 controles publicándose inicialmente en inglés y en francés tras su acuerdo de publicación el 25 de septiembre de 2013" [5]. Esta norma aún no ha sido adoptada en El Salvador.

3.1.1.4. ISO/IEC 27003

"Publicada el 01 de febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de

[5] *http://www.iso27000.es/iso27000.html*

implantación"[6]. Adoptada en El Salvador en fecha 20 de marzo de 2015 bajo el nombre NTS ISO/IEC 27003:2010.

3.1.1.5. ISO/IEC 27004

"Publicada el 15 de diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001"[6]. Adoptada en El Salvador en fecha 20 de marzo de 2015 bajo el nombre NTS ISO/IEC 27004:2009

3.1.1.6. ISO/IEC 27005

4 de junio de 2008. No certificable. Se puede decir que es un apoyo a los conceptos generales que se especifican en la ISO/IEC 27001, y ha sido diseñada para aplicar y brindar las directrices para realizar de forma satisfactoria la seguridad de la información basada en un enfoque de gestión de riesgos. Esta norma puede ser aplicada en cualquier organización que desee gestionar todos los riesgos que se puedan dar en temas de seguridad de la información.

3.1.1.7. ISO/IEC 27006

"Publicada en primera edición el 1 de marzo de 2007. Especifica los requisitos para la acreditación de entidades de auditorías y certificación de sistemas de gestión de seguridad de la información. Esta norma se trata de una versión revisada de la EA-7/03 (requisitos para la acreditación de entidades) que añade a la ISO/IEC 17021 (requisitos para entidades de auditoría y certificación de Sistemas de Gestión), los requisitos específicos de la ISO/IEX 27001 y los del Sistema de Gestión de Seguridad de la Información. Asimismo, esta norma nos facilita y ayuda a interpretar todos los criterios de acreditación de ISO/IEC 17021 cuando se aplican en organismos de certificación de la norma ISO/IEC 27001, pero no se trata de una norma de acreditación por sí misma"[6]. Adoptada en El Salvador en fecha 20 de marzo de 2015 bajo el nombre NTS ISO/IEC 27006:2011

3.1.1.8. ISO/IEC 27007

Es un manual de auditoría de un Sistema de Gestión de Seguridad de la Información. Es un estándar Internacional el cual ha sido creado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).ISO/IEC 27008

[6] *http://www.iso27000.es/iso27000.html*

3.1.1.9. ISO/IEC 27008

Es un estándar que suministra orientación acerca de la implementación y operación de los controles. Es compatible con otras normas como la ISO/IEC 27001 O ISO/IEC 27002 y sirve como plataforma estratégica para la garantizar la seguridad de la información. Soporta tanto la planificación como la ejecución del SGSI y el proceso de gestión del riesgo del sistema de la organización.

La norma incluye la comprobación de la conformidad técnica frente a un estándar de implementación de seguridad de la información establecido en la empresa. No busca suministrar orientaciones específicas sobre la verificación del cumplimiento relativo a la medición, evaluación del riesgo o auditoría del SGSI.

3.1.1.10. ISO/IEC 27009

"No certificable. Es una guía sobre el uso y aplicación de los principios de ISO/IEC 27001 para el sector servicios específicos en emisión de certificaciones acreditadas de tercera parte"[7].

3.1.1.11. ISO/IEC 27010

"Publicada el 20 de octubre de 2012. Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. ISO/IEC 27010:2012 es aplicable a todas las formas de intercambio y difusión de información sensible, tanto pública como privada, a nivel nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores. En particular, puede ser aplicable a los intercambios de información y participación en relación con el suministro, mantenimiento y protección de una organización o de la infraestructura crítica de los estados y naciones"[7].

3.1.1.12. ISO/IEC 27011

"Publicada el 15 de Diciembre de 2008. Consiste en una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002:2005"[7].

3.1.1.13. ISO/IEC 27012

"Comprende un conjunto de requisitos y directrices de gestión de seguridad de la información en todas aquellas organizaciones que ofrezcan servicios de e-Administración"[8].

[7] *http://www.iso27000.es/iso27000.html*

3.1.1.14. ISO/IEC 27013

"Publicada el 15 de Octubre de 2012. Consiste en una guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 2000-1 (gestión de servicios TI)"[9].

3.1.1.15. ISO/IEC 27014

"Publicada el 23 de Abril de 2013. Consistirá en una guía de gobierno corporativo de la seguridad de la información"[9].

3.1.1.16. ISO/IEC 27015

"Publicada el 23 de Noviembre de 2012. Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros"[9].

3.1.1.17. ISO/IEC 27016

"Consistirá en una guía de gobierno corporativo de la seguridad de la información"[9].

3.1.1.18. ISO/IEC 27017

"Consistirá en una guía de seguridad para el Cloud Computing"[10].

3.1.1.19. ISO/IEC 27018

"Consistirá en un código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing"[10].

3.1.1.20. ISO/IEC 27019

"Publicada el 17 de Julio de 2013. Es una guía con referencia a ISO/IEC 27002:2005 para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía"[10].

3.1.1.21. ISO/IEC 27031

"Publicada el 1 marzo de 2011. Describe los conceptos y principios de la tecnología de información y comunicaciones (TIC), no es certificable, además consiste en una guía de apoyo para la continuidad de negocio y la descripción de los procesos y métodos necesarios para señalar e identificar todos los aspectos que sirvan para mejorar la preparación de las TIC de una empresa con la única finalidad de garantizar la continuidad de negocio"[10].

---

[8] *http://www.custodia-documental.com/familia-iso-27000-seguridad-de-la-informacion/*
[9] *http://www.custodia-documental.com/familia-iso-27000-seguridad-de-la-informacion/*
[10] *http://www.iso27000.es/iso27000.html*

3.1.1.22. ISO/IEC 27032

"Publicada el 16 de Julio de 2012. Proporciona orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad. Esta norma establece una descripción general de Seguridad Cibernética, una explicación de la relación entre la ciberseguridad y otros tipos de garantías, una definición de las partes interesadas y una descripción de su papel en la seguridad cibernética, una orientación para abordar problemas comunes de Seguridad Cibernética y un marco que permite a las partes interesadas a que colaboren en la solución de problemas en la ciberseguridad"[11].

3.1.1.23. ISO/IEC 27033

"Es una norma derivada de la norma de seguridad ISO/IEC 18028 de la red. Esta norma da una visión general de seguridad de la red y de los conceptos asociados. Explica las definiciones relacionadas y aporta orientación de la gestión de la seguridad de la red"[12].

Consiste en 7 partes:

- Gestión de seguridad de redes
- Arquitectura de seguridad de redes
- Marcos de redes de referencia
- Aseguramiento de las comunicaciones entre redes mediante gateways
- Acceso remoto
- Salvaguardia de comunicaciones en redes mediante VPNs
- Diseño e implementación de seguridad en redes.

3.1.1.24. ISO/IEC 27034

"Esta norma está dedicada a la seguridad en aplicaciones informáticas, consistente en 6 partes: 27034-1, conceptos generales; 27034-2, marco normativo de la organización; 27034-3, proceso de gestión de seguridad en aplicaciones; 27034-4, validación de la seguridad en aplicaciones; 27034-5, estructura de datos y protocolos y controles de seguridad de aplicaciones; 27034-6, guía de seguridad para aplicaciones de uso específico"[11].

[11] *http://www.iso27000.es/iso27000.html*
[12] *http://www.pmg-ssi.com/2014/04/iso-27033-seguridad-en-la-red/*

3.1.1.25. ISO/IEC 27035

"Publicada el 17 de agosto de 2011. Proporciona una guía sobre la gestión de incidentes de seguridad en la información"[13].

3.1.1.26. ISO/IEC 27036

"Guía en cuatro partes de seguridad en las relaciones con proveedores y/o outsourcing: 27036-1, visión general y conceptos; 27036-2, requisitos comunes; 27036-3, seguridad en la cadena de suministro TIC; 27036-4, seguridad en entornos de servicios Cloud"[13].

3.1.1.27. ISO/IEC 27037

"Publicada el 15 de Octubre de 2012. Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones"[13].

3.1.1.28. ISO/IEC 27038

"Consistirá en una guía de especificación para realizar técnicas de seguridad en la redacción digital en documentos digitales, también, especifica requerimientos para la redacción de herramientas de software y métodos de prueba donde la redacción digital tiene que estar completamente segura"[13].

3.1.1.29. ISO/IEC 27039

"Provee una guía a las organizaciones en la preparación para el despliegue sistemas de detección y prevención de intrusos (IDS /IPS)"[13]. En particular, dirige la selección, el despliegue y la operación de un IDS/IPS.

3.1.1.30. ISO/IEC 27040

"El propósito de esta norma es proveer una guía detallada de implementación de seguridad para los sistemas o medios de almacenamiento"[14].

[13] *http://www.iso27000.es/iso27000.html*
[14] *https://www.iso.org/obp/ui/#iso:std:iso-iec:27040:ed-1:v1:en*

3.1.1.31. ISO/IEC 27041

Consistirá en una guía para la garantizar la idoneidad y adecuación de los métodos de investigación.

3.1.1.32. ISO/IEC 27042

"Consistirá en una guía con directrices para el análisis e interpretación de las evidencias digitales"[15].

3.1.1.33. ISO/IEC 27043

"Desarrollará principios y procesos de investigación para la recopilación de evidencias digitales"[15].

3.1.1.34. ISO/IEC 27044

"Gestión de eventos y de la seguridad de la información - Security Information and Event Management (SIEM)"[15].

3.1.1.35. ISO/IEC 27799

"Publicada el 1 de julio de 2012. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes. Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215"[15].

3.2. Adaptación de las 4 normas

Para el presente trabajo se ha decido adaptar las normas NTS ISO/IEC 27001:2013, NTS ISO/IEC 27003:2010 y NTS ISO/IEC 27004:2009 debido a que corresponden al ciclo de Deming (Plan, Hacer, Revisar y Actuar). De dichas normas se ha retomado los conceptos, requisitos y guía de implementación para la conformación de la propuesta metodológica para la implementación, cumplimiento y medición de un SGSI a la medida de la PYME Salvadoreña. Adicionalmente se han considerado dichas normas ya que han sido adoptadas por El Salvador, excluyendo la norma 27000 por estar fuera de vigencia.

[15] *http://www.iso27000.es/iso27000.html*

4. Desarrollo del trabajo

4.1. Metodología propuesta

Metodología para la implementación, cumplimiento y medición de un SGSI a la medida de la PYME Salvadoreña.

0. Introducción

Esta metodología para la implementación, cumplimiento y medición de un SGSI a la medida de la PYME salvadoreña es una adaptación de las Normas NTS ISO/IEC 27001:2013, NTS ISO/IEC 27003:2010 e NTS ISO/IEC 27004:2009 a los requerimientos de seguridad de la PYME. Esta propuesta permitirá a cualquier organización de éste tipo gestionar, evaluar y medir la seguridad de sus sistemas de información. El desarrollo de ésta propuesta se basa en un estudio realizado en empresas PYME de diferentes sectores del país, en las cuales a partir de una encuesta se identificó un alto grado de riesgos asociados con la confidencialidad, integridad y disponibilidad de la información.

Las pequeñas y medianas empresas que implementan las normas NTS ISO/IEC 27001:2013, NTS ISO/IEC 27003:2010 y NTS ISO/IEC 27004:2009 pueden alcanzar los mismos resultados exitosos que las organizaciones más grandes. No obstante, es importante señalar que la PYME podría contar con presupuesto limitado y menos tiempo para gestionar los riesgos de seguridad de la información. Es por ello que la adaptación de las normas de la familia ISO/IEC 27000 ofrece a las empresas la posibilidad de eliminar costos innecesarios y reducir la complejidad de los requisitos de dicha normativa. La metodología desarrollada pretende generar una configuración de seguridad óptima para las PYMES pero no necesariamente la mejor, priorizando los tiempos de implantación y ahorro de costos frente a la precisión, garantizando que los resultados obtenidos brinden la calidad y eficiencia suficiente.

Algunos de los beneficios que se espera que la PYME pueda alcanzar con la implementación de ésta propuesta son: el incremento de eficiencia, el aumento de la credibilidad tanto en la empresa como en los productos, el aumento de la confianza que los clientes tienen en la empresa y la posibilidad de la apertura de nuevos mercados nacionales e internacionales.

Tomando como base lo anterior y a partir de la información obtenida, se ha desarrollado una metodología para un SGSI en las PYMES de EL Salvador y un modelo asociado de la misma, tal como se muestra en la siguiente figura:

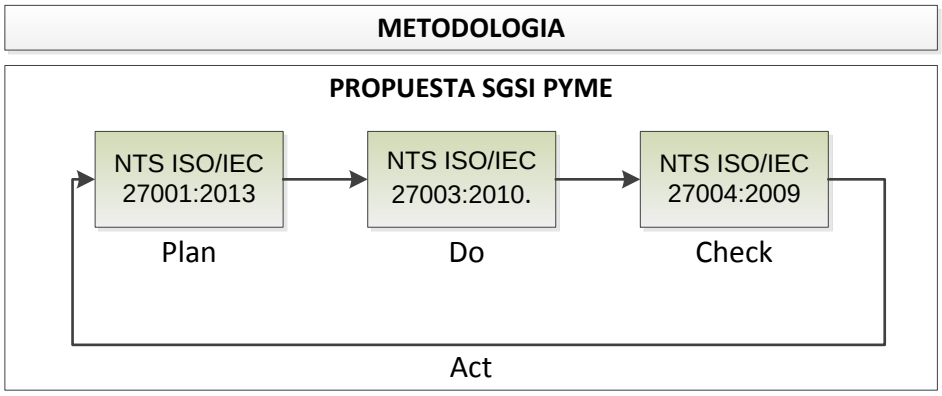

Figura 1. Procesos de la metodología propuesta

Plan (establecimiento del SGSI)	•Establecer la política, objetivos, procesos y procedimientos del SGSI pertinentes a la gestión de riesgo y mejorar la seguridad de la información para obtener resultados de acuerdo con las políticas y objetivos generales de la organización.
Hacer (implementación y operación del SGSI)	•Implementar y operar la política, controles, procesos y procedimientos del SGSI.
Verificar (supervisión y revisión del SGSI)	•Evaluar y medir el rendimiento del proceso contra la política, los objetivos y la experiencia práctica del SGSI, e informar de los resultados a la Dirección para su revisión.
Actuar (mantenimiento y mejora del SGSI)	•Tomar acciones correctivas y preventivas, basadas en los resultados de auditorías internas del SGSI y de revisión de gestión u otra información relevante, para lograr la mejora continua del SGSI.

1. Alcance

Ésta metodología para la implementación, cumplimiento y medición de un SGSI a la medida de la PYME, establece además los requerimientos para la evaluación y tratamiento de riesgos de seguridad de la información de acuerdo a las necesidades y tamaño de la empresa.

Los requerimientos propuestos son de carácter genérico y tiene la intensión de brindar una guía para su implementación en cualquier PYME sin importar el tamaño, tipo o sector al que pertenezca.

2. Referencias normativas

Los siguientes documentos, en forma completa o en parte, son referenciados normativamente en éste documento y son indispensables para su aplicación. Se aplica la versión del documento indicada.

NTS ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requerimientos.

NTS ISO/IEC 27003:2010. Tecnología de la información. Técnicas de seguridad. Guía de implementación del sistema de gestión de la seguridad de la información.

NTS ISO/IEC 27004:2009. Tecnología de la información. Técnicas de seguridad. Gestión de seguridad de la información. Medición.

3. Términos y definiciones

- Dirección: se refiere a la más alta persona que tome decisiones en la empresa.
- Para propósitos de éste documento se aplican los términos y definiciones dados en ISO/IEC 27000
- Para propósitos de éste documento se aplican los términos y definiciones dados en NTS ISO/IEC 27001:2013.

4. Requisitos a cumplir

4.1 Requisitos generales

La organización establecerá, implementará, operará, monitoreará, revisará, mantendrá y mejorará un SGSI organizado en su contexto de sus actividades empresariales y de los riesgos que ésta afronta. Para éste propósito, el proceso ésta basado en el modelo PDCA, presentado en la figura 1.

4.2 Comprensión de la organización y su contexto

La empresa debe determinar los asuntos internos y externos dentro de su contexto que son relevantes a su misión y que afectan su habilidad para alcanzar los resultados esperados de su Sistema de Gestión de Seguridad de la Información.

Debe considerarse: la misión de la empresa, los valores, el sector en que se desarrolla y las características propias de la misma. Objetivos y prioridades respecto al desarrollo del negocio, planes de continuidad del mismo.

Para los casos en que las empresas no posean una Misión definida, se puede tomar en cuenta como parte de ésta, lo que el dueño considere como la razón de ser de la empresa.

4.3 Comprensión de las necesidades y expectativas de las partes interesadas

Es fundamental que la empresa determine las partes interesadas tanto al interior como al exterior de la empresa, ambos son relevantes para el sistema de gestión de seguridad de la información. Los requerimientos legales, regulatorios y obligaciones contractuales para la seguridad de la información.

4.4 Determinar el alcance del SGSI

Es decir, la empresa debe determinar sobre qué proceso o procesos va proceder, debe tomar en cuenta que la implementación en toda la entidad no es necesaria. Debe evaluar los recursos que se pueden dedicar para el proyecto y determinar si realmente es necesario abarcar toda la empresa en dicho esfuerzo. Por lo general resulta más práctico limitar el alcance del SGSI a los servicios o procesos en los que resulte más sencillo. Lograr dimensionar el proyecto en proporciones reales es fundamental para alcanzar el éxito.

Por tanto, la empresa debe establecer un alcance y los límites del SGSI en términos de las características de la actividad empresarial de la empresa, sus activos, su tecnología, incluyendo los detalles y justificación de cualquier exclusión del alcance.

El alcance deberá determinarse en función de:

a) Los asuntos internos y externos referidos en el 4.2
b) Los requerimientos referidos en el 4.3
c) Las interconexiones y dependencias entre las actividades que se desempeñan al interior de la empresa y aquellas que son desempeñadas por otras organizaciones.

El alcance debe documentarse y debe estar disponible como referencia de consulta y ser de conocimiento de los interesados.

4.5 Sistema de Gestión de la Seguridad de la Información

La empresa debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la información.

4.6 Liderazgo y compromiso

Una exigencia para la implementación de un SGSI es contar con el compromiso de la Dirección, no solo por ser un requisito contemplado en la norma, sino porque su apoyo y respaldo tanto en recursos como en la generación de un cambio de cultura empresarial son fundamentales para el éxito del proyecto.

La dirección debe hacer evidente su involucramiento con el establecimiento, implementación, monitorización, revisión, mantenimiento y mejora continua del SGSI. La forma en que se hace evidente éste compromiso es asistiendo o ejecutando las siguientes tareas:

a) Establecer la política del SGSI

b) Asegurar que se establecen los objetivos y planes del SGSI y que son compatibles con la empresa.
c) Asignar los recursos suficientes para crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.
d) Comunicar a todo el personal e interesados, la importancia del cumplimiento de los objetivos de seguridad de la información y de acuerdo a la política de seguridad de la información, las responsabilidades legales y la necesidad de la mejora continua.
e) Asignar los roles y responsabilidades para la seguridad de la información.
f) Decidir los criterios de aceptación del riesgo
g) Dirigir y apoyar a las personas que contribuyen a la efectividad del SGSI.
h) Verificar que se realizan las auditorías internas y externas del SGSI.
i) Promover la mejora continua.
j) Dirigir la gestión de las revisiones del SGSI.

4.7 Política de Seguridad de Gestión de la Información

La política de seguridad debe recoger las líneas generales de actuación de la empresa en un documento que estará firmado por la dirección, en dicho documento deberá evidenciarse el compromiso por velar por la confidencialidad, integridad y disponibilidad de los activos de información.

La dirección debe definir una política de seguridad de la información de acuerdo a las características del negocio, su organización, sus activos y a la tecnología, ésta política debe:

a) Ser apropiada para el propósito de la empresa
b) Proveer un marco para establecer los objetivos de seguridad de la información
c) Tener en cuenta los requisitos de la actividad empresarial, los requisitos legales o reglamentarios y las obligaciones de seguridad contractuales;
d) Incluir un compromiso para satisfacer los requerimientos aplicables relacionados a la seguridad de la información
e) Incluir un compromiso con la mejora continua.
f) Estar aprobada por la dirección
g) Estar divulgada

La política de seguridad de la información debe estar disponible como información documental, ser comunicada dentro de la organización y estar disponible a las partes interesadas, de manera apropiada.

4.8 Roles, responsabilidades y autoridades organizacionales

La dirección debe asegurar que el rol relevante a la seguridad de la información y sus responsabilidades, sea asignado y comunicado a las partes interesadas.

La dirección debe asignar la responsabilidad y autoridad para:

a) Asegurar que el sistema de gestión de la seguridad de la información esté conforme a ésta metodología.
b) Mantener informada a la dirección sobre el desempeño del sistema de gestión de seguridad de la información.

Nota: Cuando se requiera, la dirección puede también asignar responsabilidades y autoridades para informar el desempeño del sistema de gestión de seguridad de la información.

4.9 Planeación

4.9.1 Acciones a abordar riesgos y oportunidades

4.9.1.1 General

Cuando se esté planeando para el SGSI, la empresa debe considerar los elementos referidos en el 4.3 y los requerimientos referidos en el 4.4 y determinar los riesgos y oportunidades que necesitan ser abordados para:

a) Asegurar que el SGSI pueda obtener los resultados esperados
b) Prevenir o reducir los efectos no deseados
c) Lograr la mejora continua

La organización debe planear:

d) Acciones para abordar estos riesgos y oportunidades
e) Como:
    1. Integrar e implementar las acciones dentro de los procesos del SGSI
    2. Evaluar la efectividad de estas acciones

4.9.1.2 Evaluación del riesgo de seguridad de la información

La dirección debe definir y aplicar un proceso de evaluación del riesgo de seguridad de la información que:

a) Establezca y mantenga criterios de riesgo de seguridad de la información que incluyan:
    1. El criterio de aceptación del riesgo
    2. Criterio de desempeño de la evaluación de riesgo de seguridad de la información
b) Asegure que repetidas evaluaciones de riesgo de seguridad de la información producen resultados consistentes, válidos y comparables
c) Identifique los riesgos de seguridad de la información
    1. Aplica el proceso de evaluación de riesgo de seguridad de la información para identificar riesgo asociados con la pérdida de la confidencialidad, integridad y disponibilidad para los activos de información dentro del alcance del SGSI.
    2. Identifica los propietarios del riesgo
d) Analice los riesgos de seguridad de la información
    1. Evalúa las potenciales consecuencias que pueden resultar si se materializan los riesgos identificados
    2. Evalúa la posibilidad real de ocurrencia de los riesgos identificados
    3. Determina los niveles de riesgo
e) Evalúe los riesgos de seguridad de la información
    1. Compara los resultados del análisis de riesgo contra el criterio establecido
    2. Prioriza los riesgos analizados para el tratamiento del riesgo

La empresa debe conservar información documental acerca del proceso de evaluación del riesgo de seguridad de la información.

4.9.1.3 Tratamiento del riesgo de seguridad de la información

La empresa debe definir y aplicar un proceso de tratamiento del riesgo de seguridad de la información para:

a) Seleccionar opciones apropiadas para el tratamiento del riesgo de seguridad de la información, tomando en cuenta los resultados de la evaluación del riesgo
b) Determinar los controles que son necesarios para implementar las opciones seleccionadas para el tratamiento del riesgo de seguridad de la información.
c) Comparar los controles determinados en con los del apartado 5 “Guía de implementación, métricas y mediciones” y verificar que no han sido omitidos como controles necesarios

d) Generar una declaración de aplicabilidad que contenga los controles necesarios y la justificación para inclusiones, ya que sean implementadas o no, y la justificación de exclusiones de control del apartado 5 “Guía de implementación, métricas y mediciones”
e) Formularia un plan de tratamiento de riesgo de seguridad de la información
f) Obtener aprobación del plan de tratamiento del riesgo de seguridad de la información y aceptación de los riesgos residuales por parte de los propietarios del riesgo

La empresa debe retener la información documental acerca del proceso de tratamiento de riesgo de seguridad de la información.

4.9.2 Objetivos de seguridad de la información y planeación para lograrlos

La organización debe establecer objetivos de seguridad de la información en niveles y funciones pertinentes.

Los objetivos de seguridad de la información deben:

a) Ser consistentes con la política de seguridad de la información
b) Ser medibles
c) Tomar en cuenta los requerimientos aplicables a la seguridad de la información, y a los resultados de la evaluación y tratamiento del riesgo
d) Ser comunicados
e) Ser actualizados apropiadamente

La empresa debe conservar información documental sobre los objetivos de seguridad de la información.

Cuando se planee como alcanzar los objetivos de seguridad de la información, la organización debe determinar:

f) Que será realizado
g) Que recursos serán requeridos
h) Quién será el responsable
i) Cuándo se completará
j) Cuando se evaluarán los resultados

4.10 Soporte

4.10.1 Recursos

La empresa debe determinar y proveer los recursos necesarios para el establecimiento, implementación, mantenimiento y la mejora continua del sistema de gestión de seguridad de la información.

4.10.2 Competencia

La empresa debe:

a) Determinar la competencia necesaria de las personas desarrollando trabajos bajo su control que afectan el desempeño de la seguridad de la información
b) Asegurar que estas personas son competentes sobre la base de una educación, entretenimiento o experiencia apropiada.
c) Donde sea aplicable, tomar acciones para adquirir las competencias necesarias y evaluar la efectividad de las acciones tomadas
d) Retener la información documental apropiada como evidencia de la competencia

4.10.3 Conciencia

Las personas desarrollando trabajo bajo el control de la empresa deben estar conscientes de:

a) La política de seguridad de la información
b) Su contribución a la efectividad del sistema de gestión de seguridad de la información, incluyendo los beneficios del desempeño mejorado de seguridad de la información.
c) Las implicaciones de no conformidad con los requerimientos del sistema de gestión de seguridad de la información.

4.10.4 Comunicación

La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al SGSI que incluyan:

a) Qué comunicar
b) Cuándo comunicar
c) A quién comunicar
d) Quién debe comunicar
e) Los procesos por los cuales la comunicación debe ser efectuada

4.10.5 Información documental

4.10.5.1 General

El sistema de gestión de seguridad de la información de la organización debe incluir:

a) Información documental requerida por la norma NTS ISO/IEC 27001:2013
b) Información documental determinada por la organización como necesaria para la efectividad del sistema de gestión de seguridad de la información.
    1. El tamaño de la organización y su tipo de actividades, procesos, productos y servicios
    2. La complejidad de los procesos o sus interacciones
    3. Las competencias de las personas.

4.10.5.2 Creación y actualización

Cuando se cree y actualice información documental, la organización debe asegurar su propia

a) Identificación y descripción (por ejemplo: un título, fecha, autor o número de referencia)
b) Formato (por ejemplo: lenguaje, versión de software, gráficos) y medio (por ejemplo: papel, electrónico)
c) Revisión y aprobación para su idoneidad y adecuación.

4.10.5.3 Control de información documental

La información documental requerida por SGSI debe ser controlada para asegurar:

a) Que esté disponible y sea idónea para su uso, donde y cuando sea necesario
b) Esté adecuadamente protegida (por ejemplo: de pérdida de confidencialidad, uno inapropiado o pérdida de integridad)
c) Distribución, acceso, recuperación y uso
d) Almacenamiento y conservación, incluyendo la conservación de la legibilidad
e) Control de cambios (por ejemplo: control de versiones)
f) Retención y disposición

La información documental de origen externo, determinada por la organización como necesaria para la planificación y operación del SGSI, debe ser oportunamente identificada y controlada.

4.11 Operación

4.11.1 Planeación y control operacional

La empresa debe planificar, implementar y controlar los procesos necesarios para cumplir los requerimientos de seguridad de la información, y para implementar las acciones determinadas en 4.9.1. La organización también debe implementar planes para lograr los objetivos de la seguridad de la información determinados en 4.9.2.

La empresa debe mantener información documental en la medida necesaria que proporcione la confianza que los procesos han sido ejecutados como fueron planeados.

La empresa debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acción para mitigar cualquier efecto adverso donde sea necesario.

La empresa debe asegurar que los procesos sub contratados estén determinados y controlados.

4.11.2 Evaluación de riesgo de seguridad de la información

La empresa debe desarrollar evaluaciones de riesgo de seguridad de la información planificadas periódicamente o cuando ocurran o sean propuestos cambios significativos, tomando en cuenta el criterio establecido en 4.9.1.2 a).

La empresa debe retener información documental de los resultados de las evaluaciones del riesgo de seguridad de la información.

4.11.3 Tratamiento del riesgo de seguridad de la información

La empresa debe implementar el plan de tratamiento del riesgo de seguridad de la información.

La organización debe retener información documental de los resultados del tratamiento del riesgo de seguridad de la información.

4.12 Evaluación del desempeño

4.12.1 Monitoreo, medición, análisis y evaluación

La empresa debe evaluar el desempeño de la seguridad de la información y la efectividad del sistema de gestión de seguridad de la información.

La empresa debe determinar:

a) Qué necesita ser monitoreado y medido, incluyendo procesos y controles de seguridad de la información
b) Los métodos para monitorear, medir, analizar y evaluar, según sean aplicables para asegurar la validez de los resultados.
c) Cuando el monitoreo y la medición deben ser ejecutados
d) Quién debe monitorear y medir
e) Cuándo los resultados del monitoreo y la medición deben ser analizados y evaluados
f) Quién debe analizar y evaluar estos resultados

La empresa debe retener información documental apropiada como evidencia de los resultados del monitoreo y revisión.

4.12.2 Auditoría interna

La empresa deberá ejecutar auditorías internas planificadas periódicamente para proveer información sobre si el SGSI:

a) Está conforme a los requerimientos propios de la organización para su SGSI.
b) Es efectivamente implementado y mantenido
c) Definir el criterio de auditoría y el alcance para cada auditoría.
d) Seleccionar los auditores y ejecutar auditorías que aseguren la objetividad e imparcialidad del proceso de auditoría
e) Asegurar que los resultados de las auditorías son informados a la administración pertinente
f) Retener información documental como evidencia del o de los programas de auditoría y los resultados de la auditoría.

4.12.3 Revisión por la Dirección

La Dirección de la empresa, debe revisar el SGSI de la empresa a períodos planificados para asegurar su continua idoneidad, adecuación y efectividad.

La revisión de la dirección debe incluir consideraciones de:

a) El estado de acciones de previas revisiones de la Dirección
b) Cambios en asuntos internos y externos que sean relevantes al SGSI
c) Retroalimentación de partes interesadas
d) Resultados de evaluación de riesgo y estado del plan de tratamiento de riesgos
e) Oportunidades de mejora continua.

Los resultados de ésta revisión deben incluir decisiones relacionadas a oportunidades de mejora continua y cualquier necesidad de cambios del sistema de gestión de seguridad de la información.

La organización debe retener información documental como evidencia de los resultados de ésta revisión.

4.13 Mejora

4.13.1 Incumplimiento y acción correctiva

Cuando un incumplimiento ocurre, la empresa debe:

a) Reaccionar al incumplimiento, y según aplique:
    1. Tomar acción para controlarla y corregirla
    2. Lidiar con las consecuencias
b) Evaluarla necesidad de acciones para eliminar las causas del incumplimiento, de tal forma que esta no sea recurrente o se de en otros lugares, a través de:
    1. Revisar el incumplimiento
    2. Determinar las causas del incumplimiento
    3. Determinar si existen causas similares que causaron el incumplimiento o podría ocurrir potencialmente
c) Implementar cualquier acción necesaria
d) Revisar la efectividad de cualquier acción necesaria
e) Realizar cambios al SGSI de ser necesario

Las acciones correctivas deben corresponder a los efectos de las no conformidades encontradas. La empresa debe retener información documental como evidencia de:

f) La naturaleza del incumplimiento y cualesquiera sean las acciones subsecuentes tomadas

g) Los resultados de cualquier acción correctiva

4.14 Mejora continua

La empresa debe continuamente mejorar la idoneidad, adecuación y efectividad del SGSI

5. Guía de implementación, métricas y mediciones

Ref.	***Control***	**Descripción (objetivo)**	**Actividad**	**Criterio de aplicabilidad**	**Medición**	**Consejos para implementación**
1. Política de seguridad de la información						
1.1	*Política para la seguridad de la información*	Un conjunto de políticas de seguridad de la información debe ser definido y aprobado por la dirección, publicarlo y comunicarlo a todos los empleados y entidades externas pertinentes	La política del SGSI debería ser desarrollada y la aprobación de la Dirección debería ser obtenida	**Requerido**	Cobertura de la política (es decir, porcentaje de secciones de NTS ISO/IEC 27001:2013 para las cuales se han especificado, escrito, aprobado y publicado políticas y sus normas, procedimientos y directrices asociadas. Grado de despliegue y adopción de la política en la organización (medido por auditoría, gerencia o auto-evaluación).	Se debe elaborar la política en base a la información y conocimiento adquirido o identificado por la Dirección como importante en un análisis previo. Piense en términos de un manual de políticas de seguridad de la información que contenga un conjunto coherente e internamente consistente de políticas, normas, procedimientos y directrices.
1.2	*Revisión de la política para la seguridad de la información*	La política para la seguridad de la información debe revisarse periódicamente o siempre que se produzcan cambios significativos, para asegurar que se mantenga su continuidad, idoneidad, adecuación y efectividad.	Se debería de desarrollar un plan para asegurar que la Dirección participe y se comprometa en la revisión de la operación y mejoramiento continuo del SGSI	**Requerido**	Número y versiones en las revisiones de la política, en las cuales se puede realizar mejoras, actualización, sobre forma y contenido de la misma en base a los requerimientos de negocio	La política para la seguridad de la información debe revisarse periódicamente o siempre que se produzcan cambios significativos, para asegurar que se mantenga su continuidad, idoneidad, adecuación y efectividad.

2. Organización de la seguridad de la información						
2.1	*Organización interna*	Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización	La funciones, roles y responsabilidades organizacionales para la seguridad de la información deberían estar alineadas con el tratamiento del riesgo	**Requerido**	Porcentaje de funciones/unidades organizativas para las cuales se ha implantado una estrategia global para mantener los riesgos de seguridad de la información por debajo de umbrales explícitamente aceptados por la dirección. Porcentaje de empleados que han recibido y aceptado formalmente, roles y responsabilidades de seguridad de la información	La estructura organizacional diseñada para el SGSI debería reflejar las actividades para la implementación y operación del SGSI, definiendo roles y responsables para la seguridad de la información, así como también, debe existir una segregación de funciones y un adecuado contacto con las autoridades pertinentes. Reproduzca la estructura y tamaño de otras funciones corporativas especializadas, como Legal, Riesgos y Complimiento
2.2	*Dispositivos móviles y trabajo remoto*	Asegurar la seguridad del trabajo remoto y el uso de dispositivos móviles	Se debería definir e implementar una política de seguridad, en donde se establezca y se adopte medidas para gestionar cualquier tipo de riesgo introducido por el uso de dispositivos móviles, asi como también, se debe establecer medidas de seguridad para proteger la información accedida y procesada desde sitios remotos.	**Recomendable**	"Estado de la seguridad en entorno portátil / teletrabajo", es decir, un informe sobre el estado actual de la seguridad de equipos informáticos portátiles (laptops, PDAs, teléfonos móviles, etc.), y de trabajo remoto (en casa de los empleados), con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, despliegue de configuraciones seguras, antivirus, firewalls, personales, etc.	Tenga políticas claramente definidas para la protección, no sólo de los propios equipos informáticos portátiles (es decir, laptops, PDAs, etc.), sino, en mayor medida, de la información almacenada en ellos. Por lo general, el valor de la información supera con mucho el del hardware. Asegúrese de que el nivel de protección de los equipos informáticos utilizados dentro de las instalaciones de la organización tiene su correspondencia en el nivel de protección de los equipos portátiles, en aspectos tales como antivirus, parches, actualizaciones, software cortafuegos, etc.
3. Seguridad de los recursos humanos						
3.1	*Antes del empleo*	Asegurar que los empleados y contratistas entiendan sus responsabilidades, y sean idóneos para los roles para los cuales se les considera	Las verificaciones para la selección de personal debería llevarse acorde a las leyes, regulaciones y normas de ética pertinentes, y deben ser proporcionales al requerimiento del negocio, la clasificación de la información y los riesgos percibidos	**Requerido**	Porcentaje de nuevos empleados o pseudo-empleados (contratistas, consultores, temporales, etc.) que hayan sido totalmente verificados y aprobados de acuerdo con las políticas de la empresa antes de comenzar a trabajar.	En conjunto al área de Recursos Humanos o el área responsable de la contratación del recurso humano, asegure que se emplea un proceso de verificación de antecedentes proporcional a la clasificación de seguridad de aquella información a la que va a acceder el empleado a contratar. Dicho simplemente, el proceso de contratación de un administrador de sistemas TI debería ser muy diferente del de un administrativo. Haga comprobaciones de procedencia, formación, conocimientos, etc.

3.2	*Durante el empleo*	Asegurar que todos los empleados y contratistas estén conscientes de cumplir con sus responsabilidades de la seguridad de la información	La dirección debe requerir a los empleados y/o contratistas aplicar todas las políticas y procedimientos de seguridad de la información y hacer ver la existencia de un proceso disciplinario ante cualquier violación de las mismas, así como también, deberían de existir capacitaciones sobre la concientización del cumplimiento de dichas políticas	**Requerido**	Respuesta a las actividades de concienciación en seguridad medidas por, p. ej., el número de e-mails, llamadas, asistentes a charlas relativas a iniciativas de concientización	La responsabilidad con respecto a la protección de la información no finaliza cuando un empleado se va a casa o abandonala organización. Asegure que esto se documenta claramente en materiales de concienciación, contratos de empleo, etc.Contemple la posibilidad de una revisión anual por RRHH o el área responsable de gestionar el recurso humano de los contratos junto con los empleados para refrescar las expectativas expuestas en los términos y condiciones de empleo, incluyendo su compromiso con la seguridad de la información.Asegúrese de que exista un proceso disciplinario que tome acción en contra de empleados o terceros que cometan una violación en la seguridad de la información.
3.3	*Terminación y cambio del empleo*	Proteger los interese de la organización como parte de un proceso de terminación o cambio de empleo.	Deberían ser definidas las responsabilidades y funciones de la seguridad de la información que permanezcan validas después de una terminación o cambio de empleo, comunicadas al empleado o contratista	**Recomendable**	Porcentaje de identificadores de usuarios de sistemas pertenecientes a personas que han dejado la organización o han cambiado de funciones dentro la organización, separados por las categorías de activos (pendientes de desactivación) e inactivos (pendientes de archivo y borrado)	La devolución de los activos de la organización cuando un empleado se marcha sería mucho más sencilla de verificar si el inventario de activos ha sido actualizado y verificado regularmente. Examine qué accesos necesita revocar en primer lugar cuando un empleado presenta su carta de renuncia: ¿cuáles son los sistemas más críticos o vulnerables? Haga un seguimiento del uso del e-mail por estas personas antes de salir definitivamente de la empresa, por si comienzan a sacar información confidencial (sujeto a las políticas aplicables y a consideraciones legales sobre privacidad).

4. Gestión de activos						
4.1	*Responsabilidad sobre los activos*	Identificar los activos organizacionales y definir las apropiadas responsabilidades de protección	Debería existir un inventario e identificación de activos que soportan la información y serán respaldados por el SGSI, además se debe especificar, la propiedad, uso aceptable y devolución de los mismos.	**Requerido**	Porcentaje de activos de información en cada fase del proceso de clasificación (identificado / inventariado / propietario asignado / riesgo evaluado / clasificado / asegurado). Porcentaje de activos de información claves para los cuales se ha implantado una estrategia global para mitigar riesgos de seguridad de la información según sea necesario y para mantener dichos riesgos en niveles aceptables	Elabore y mantenga un inventario de activos de información, mostrando los propietarios de los activos (directivos o gestores responsables de proteger sus activos) y los detalles relevantes (p. ej., ubicación, nº de serie, nº de versión, estado de desarrollo / pruebas / producción, etc.). Use códigos de barras para facilitar las tareas de realización de inventario y para vincular equipos de TI que entran y salen de las instalaciones con empleados Para identificar los activos dentro del alcance del SGSI, se debería identificar el nombre único del proceso, descripción del proceso y actividades relacionadas, ponderación del proceso para la organización, propietarios del proceso, aplicaciones de TI que respaldan al proceso, clasificación de la información
4.2	*Clasificación de la información*	Asegurar que la información reciba un nivel apropiado de protección en concordancia con su importancia para la organización	Se debería de clasificar la información en términos de su valor, requerimiento legal, sensibilidad y criticidad, esta debería ser etiquetada en concordancia con el esquema de clasificación de la información.	**Requerido**	Porcentaje de activos de información en cada categoría de clasificación (incluida la de "aún sin clasificar")	¡Mantenga la sencillez! Distinga los requisitos de seguridad básicos (globales) de los avanzados, de acuerdo con el riesgo. Comience quizás con la confidencialidad, pero no olvide los requisitos de integridad y disponibilidad
4.3	*Manejo de medios*	Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de información almacenada en medios	Debería existir una adecuada gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización, así mismo, estos deben ser eliminados de forma segura cuando ya no sean requeridos	**Recomendable**	Porcentaje de medios removibles utilizados en la organización para el manejo de información	Tener un listado de medios removibles utilizados en la organización y definir el tipo de información que soportaran.Definir un procedimiento formal para la eliminación segura de medios cuando estos ya no son requeridos.Asegurar la protección de medios que contenga información cuando estos sean transportados

5. Control de acceso						
5.1	*Requerimiento del negocio para el control de acceso*	Limitar el acceso a la información y a instalaciones de procesamiento de la información	Se debería establecer, documentar y revisar una política de control de acceso basada en los requerimientos de seguridad de la información	**Requerido**	Porcentaje de sistemas y aplicaciones corporativas para los que los "propietarios" adecuados han: (a) sido identificados, (b) aceptado formalmente sus responsabilidades, (c) llevado a cabo -o encargado- revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y (d) definido las reglas de control de acceso basadas en roles	Los propietarios de activos de información que son responsables ante la dirección de la protección "sus" activos deberían tener la capacidad de definir y/o aprobar las reglas de control de acceso y otros controles de seguridad. Asegúrese que se les responsabilice los incumplimientos, no conformidades y otros incidentes.
5.2	*Gestión del acceso de usuarios*	Asegurar el acceso autorizado a los usuarios y prevenir el acceso no autorizado a los sistemas y servicios	La organización debe implementar un proceso formal de la gestión de acceso de usuarios, donde se especifique el proceso de altas, bajas y modificaciones de los mismos	**Requerido**	Tiempo medio transcurrido entre la solicitud y la realización de peticiones de cambio de accesos y número de solicitudes de cambio de acceso cursadas en el mes anterior (con análisis de tendencias y comentarios acerca de cualquier pico (p. ej., "Implantación de una nueva aplicación financiera este mes")	Cree la función diferenciada de "administrador de seguridad", con responsabilidades operativas para aplicar las reglas de control de acceso definidas por los propietarios de las aplicaciones y la dirección de seguridad de la información. Invierta en proporcionar al administrador de seguridad herramientas para realizar sus tareas lo más eficientemente posible
5.3	*Responsabilidades del usuario*	Hacer responsables a los usuarios por salvaguardar su información de autenticación.	Se debe de requerir a los usuarios seguir las prácticas de la organización en el uso de la información de la autenticación secreta.	**Requerido**	Porcentaje de descripciones de puesto de trabajo que incluyen responsabilidades en seguridad de la información totalmente documentadas y formalmente aceptadas.	Asegúrese de que se establecen las responsabilidades de seguridad y que son entendidas por el personal afectado. Una buena estrategia es definir y documentar claramente las responsabilidades relativas a seguridad de la información en las descripciones o perfiles de los puestos de trabajo. Son imprescindibles las revisiones periódicas para incluir cualquier cambio. Comunique regularmente a los empleados los perfiles de sus puestos (p. ej., en la revisión anual de objetivos), para recordarles sus responsabilidades y recoger cualquier cambio

5.4	*Control de acceso a sistemas y aplicaciones*	Prevenir el acceso no autorizado a sistemas y aplicaciones	Debe existir un procedimiento formal para el control de acceso a sistemas y aplicaciones, donde se definan, procedimientos seguros de acceso a la información, gestión de contraseñas, control de acceso al código fuente de los programas, etc.	**Requerido**	Porcentaje de plataformas totalmente conformes con los estándares de seguridad básica (comprobado mediante pruebas independientes), con anotaciones sobre los sistemas no conformes (p. ej., "Sistema de finanzas será actualizado para ser conforme en cuarto trimestre)"	Implante estándares de seguridad básica para todas las aplicaciones y middleware, recogiendo las mejores prácticas y checklists de CIS, NIST, fabricantes de software, etc.
6. Criptografía						
6.1	*Controles criptográficos*	Asegurar el apropiado y efectivo uso de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información	Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información, al igual que debería existir una política sobre el uso, protección y duración de las llaves criptográficas	**Recomendable**	Porcentaje de sistemas que contienen datos valiosos o sensibles para los cuales se han implantado totalmente controles criptográficos apropiados (probablemente el periodo de reporte debe ser de 3 a 12 meses)	Utilice estándares formales actuales y lo suficientemente robustos, en lugar de algoritmos de desarrollos propios.
7. Seguridad física y ambiental						
7.1	*Áreas seguras*	Prevenir el acceso físico no autorizado, daño o interferencia a las instalaciones de procesamiento de información y a la información de la organización	Se debería de establecer perímetros de seguridad para proteger áreas que contienen información, a través de controles de accesos físicos, protección de amenazas externas y ambientales, trabajo en áreas seguras, control en zonas de cargas y descargas donde cualquier persona externa puede tener acceso.	**Requerido**	Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes	Examine la entrada y salida de personas a/de su organización. ¿Hasta dónde podría llegar cualquier persona no autorizada sin ser parado, identificado y acompañado? ¿Qué podrían ver, llevarse o escuchar mientras están dentro? Algunas organizaciones usan tarjetas de identificación de colores para indicar las áreas accesibles por los visitantes (p. ej., azul para la 1ª planta, verde para la 3ª, etc.; ahora, si ve a alguien con una identificación verde en la 4º planta, reténgalo). Asegúrese de retirar todos los pases de empleado y de visita cuando se vayan. Haga que los sistemas de acceso con tarjeta rechacen y alarmen ante intentos de acceso. Use pases de visita que se vuelvan opacos o muestren de alguna manera que ya no son válidos a las x horas de haberse emitido. Haga uso de bitácoras de acceso donde se

						solicite información a las personas que por algún motivo deben accesar al centro de datos.
7.2	*Equipo*	Prevenir la perdida, daño, robo o exposición de los activos y la interrupción de las operaciones de la organización	El equipo debería de estar ubicado y protegido para reducir los riesgos de amenazas y peligros ambientales, así mismo, debería tener herramientas de soporte protegiéndolos contra fallas de energía, debería de existir un cableado seguro protegiéndolo ante cualquier intercepción, interferencia o daño. Se debe dar un adecuado mantenimiento del equipo. Al retirar activos fuera de la organización debe ser debidamente autorizados, así mismo, en la baja de equipos se debe asegurar que toda la información que pueda poseer sea eliminada de manera segura y completa.	**Requerido**	Número de chequeos (a personas a la salida y a existencias en stock) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad.	Haga que los vigilantes de seguridad impidan a cualquiera (empleados, visitas, personas de soporte TI, mensajeros, personal de mudanzas, etc.) sacar equipos informáticos de las instalaciones sin autorización escrita. Conviértalo en un elemento disuasorio visible mediante chequeos aleatorios (o, incluso, arcos de detección de metales). Esté especialmente atento a puertas traseras, rampas de carga, salidas para fumadores, etc. Tome en consideración el uso de códigos de barras para hacer los chequeos más eficientes.
8. Seguridad de las operaciones						
8.1	*Procedimientos y responsabilidades operacionales*	Asegurar la operación directa y segura de las instalaciones de procesamiento de la información	Los procedimientos realizados por operaciones debe de estar registrados y disponibles para todos los usuarios que lo necesiten.Cualquier cambio en la organización, procesos de negocios, procesamiento de la información deben ser controlados. Así mismo, el uso de recursos debe ser monitoreado y optimizado, a su vez debe de realizarse proyecciones de capacidad futuras para garantizar el buen desempeño del o los sistemas.Deberá existir una segregación de ambientes para los sistemas para reducir riesgos de accesos no autorizados o cambios en ambientes productivos.	**Recomendable**	Métricas de madurez de procesos TI relativos a seguridad, tales como el periodo de aplicación de parches de seguridad.	Documente, comunique y publique procedimientos, normas y directrices de seguridad de la información, además de roles y responsabilidades, identificadas en el manual de política de seguridad de la organización.

8.2	*Protección contra software malicioso*	Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra software malicioso	Se debería implementar controles de detección y prevención para protegerse de software malicioso y reforzarlo con una adecuada concientización del usuario	**Requerido**	Tendencia en el número de virus, gusanos, troyanos o spam detectados y bloqueados. Número y costes acumulados de incidentes por software malicioso.	Combine controles tecnológicos (p. ej., software antivirus) con medidas no técnicas (educación, concientización y formación).
8.3	*Copias de seguridad*	Permanecer protegidos contra la perdida de datos	Se deben realizar copias de seguridad de la información	**Requerido**	Porcentaje de operaciones de backup exitosas. Porcentaje de recuperaciones de prueba de backup exitosas. Tiempo medio transcurrido desde la recogida de los soportes de backup de su almacenamiento fuera de las instalaciones hasta la recuperación exitosa de los datos en todas ubicaciones principales. Porcentaje de backups y archivos con datos sensibles o valiosos que se encuentren cifrados.	Implantar procedimientos de backup y recuperación que satisfagan no sólo requisitos contractuales sino también requisitos de negocio. Básese en la evaluación de riesgos realizada para determinar cuáles son los activos de información más importantes y use esta información para crear su estrategia de backup y recuperación. Hay que decidir y establecer la estrategia y tipo de almacenamiento, frecuencia de copia y prueba de soportes. Cifre copias de seguridad y archivos que contengan datos sensibles.
8.4	*Registro y monitoreo*	Registrar eventos y generar evidencia	Se debe producir, mantener, revisar periódicamente registro de eventos, dichos registros deben ser protegidos contra acceso no deseado y/o manipulación. Se debe contar con una retención de registros según sea lo requerido por el negocio. Los sistemas de recolección e eventos de seguridad deben poseer una sincronización de reloj con una única fuente de referencia.	**Recomendable**	Porcentaje de sistemas cuyos logs de seguridad están adecuadamente configurados, son transferidos con seguridad a un sistema de gestión centralizada de logs y son monitorizados/revisados/evaluados regularmente. Tendencia en el número de entradas en los logs de seguridad que han sido registradas, han sido analizadas y han conducido a actividades de seguimiento.	Analice la criticidad e importancia de los datos que va a monitorizar y cómo esto afecta a los objetivos globales de negocio de la organización en relación a la seguridad de la información. Implemente un sistema centralizado de registros y correlación de logs de eventos de seguridad.
8.5	*Control de software operacional*	Asegurar la integridad en los sistemas operacionales	Se deben implementar procedimientos para contralar la instalación de software en sistemas operacionales	**Requerido**	Porcentaje de plataformas totalmente conformes con los estándares de instalación.	Defina controles que regulen la instalación de software. Establezca un inventario de software permitido en la organización.

8.6	*Gestión de la vulnerabilidad técnica*	Prevenir la explotación de vulnerabilidades técnicas	Se debe permanecer informado sobre las vulnerabilidades técnicas de los sistemas de información utilizados, sed debe evaluar la exposición de la organización antes estas vulnerabilidades y tomar las medidas apropiadas para abordar el riesgo asociado	**Requerido**	Duración de parchado de los sistemas (tiempo que ha llevado el parchado de al menos mitad de los sistemas vulnerables).	Haga un seguimiento constante de parches de seguridad mediante herramientas de gestión de vulnerabilidades y/o actualización automática siempre que sea posible (p. ej., Microsoft Update). Evalúe la relevancia y criticidad o urgencia de los parches en su entorno tecnológico. Pruebe y aplique los parches críticos, o tome otras medidas de protección, tan rápida y extensamente como sea posible, para vulnerabilidades de seguridad que afecten a sus sistemas y que estén siendo explotadas fuera activamente. Evite quedar fuera de soporte, debido a la obsolescencia de sus sistemas.
8.7	*Consideraciones en la auditoria de sistemas de información*	Minimizar el impacto de las actividades de auditoria en los sistemas en producción	Los requerimientos y actividades de auditoria que involucran los sistemas en producción deben ser cuidadosamente planificados y acordados para minimizar las interrupciones a los procesos de negocio	**Recomendable**	Número de recomendaciones de auditoría, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de hallazgos de auditoría relativos a seguridad de la información que han sido resueltos y cerrados, respecto al total de abiertos en el mismo periodo. Tiempo medio real de resolución/cierre de recomendaciones, respecto a los plazos acordados por la dirección al final de las auditorías.	Invierta en auditoría TI cualificada que utilice NTS ISO/IEC 27001:2013, COBIT, ITIL, CMM y estándares y métodos de buenas prácticas similares como referencias de comparación.
9. Seguridad en las comunicaciones						
9.1	*Gestión de seguridad de red*	Asegurar la protección de la información en redes y su soporte a las instalaciones de procesamiento de la información	Las redes deben ser gestionadas y controladas para proteger la información de los sistemas, así mismo, se debe identificar e incluir en acuerdos de nivel de servicio los mecanismos de seguridad, y los requisitos de gestión de todos los servicios de red. Debe de existir una segmentación de redes de acuerdo a los servicios de información, usuarios y sistemas de información	**Requerido**	Número de incidentes de seguridad de red identificados en el mes, dividido por categorías, estas pueden ser de leves, importantes o graves, con análisis de tendencias y descripción comentada de todo incidente serio y tendencia adversa.	Prepare e implante estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red.

9.2	*Transferencia de información*	Mantener la seguridad de la información que sea transferida a través de canales de comunicación de red dentro y fuera de la organización	Se deben documentar procedimientos y políticas referentes a la transferencia de información, por otro lado, deberán existir acuerdos de transferencia, confidencialidad o no divulgación de la información transmitidos a través de mensajes electrónicos o cualquier otro medio que utilice la red de datos para su transmisión	**Recomendable**	Porcentaje de enlaces de terceras partes para los cuales se han definido e implementado satisfactoriamente los requisitos de seguridad de la información.	Estudie canales de comunicaciones alternativos y "pre-autorizados", en especial direcciones de e-mail secundarias por si fallan las primarias o el servidor de correo, y comunicaciones offline por si caen las redes. El verificar canales de comunicación alternativos reducirá el estrés en caso de un incidente real.
10. Adquisición, desarrollo y mantenimiento de sistemas						
10.1	*Requisitos de seguridad de los sistemas de información*	Asegurar que la seguridad de la información sea una parte integral de los sistemas de información a través de todo su ciclo de vida	Se deberá realizar un análisis y especificación de requerimientos de seguridad de la información, se debe asegurar también los servicios de aplicación que se encuentren alojados en redes públicas, así como también, proteger las transacciones realizas dentro de estas aplicaciones	**Requerido**	Obtener un porcentaje de sistemas y aplicaciones corporativas para los que los "propietarios" adecuados han sido identificados, aceptado formalmente sus responsabilidades, llevado a cabo revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y que se encuentren definidas las reglas de control de acceso basadas en roles.	Involucre a los "propietarios de activos de información" en evaluaciones de riesgos a alto nivel y consiga su aprobación de los requisitos de seguridad que surjan. Si son realmente responsables de proteger sus activos, es en interés suyo el hacerlo bien. Esté al tanto de las novedades sobre vulnerabilidades comunes o actuales en aplicaciones e identifique e implemente las medidas protectoras o defensivas apropiadas.
10.2	*Seguridad en los procesos de desarrollo y soporte*	Asegurar que la seguridad de la información sea diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información	Se deberá realizar: una política para desarrollos seguros, procedimientos de control de cambios de sistemas, revisión técnica de las aplicaciones después de cambios en las plataformas corporativas, restricción en los cambios a los paquetes de software, principios de ingeniería de sistemas seguros, ambiente de desarrollo seguro, pruebas de seguridad del sistema, pruebas de aceptación del sistema	**Requerido**	"Estado de la seguridad en sistemas en desarrollo", es decir, un informe sobre el estado actual de la seguridad en los procesos de desarrollo de software, con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo creciente, etc.	Incorpore la seguridad de la información al ciclo de vida de desarrollo de sistemas en todas sus fases, desde la concepción hasta la desaparición de un sistema, por medio de la inclusión de "recordatorios" sobre seguridad en los procedimientos y métodos de desarrollo, operaciones y gestión de cambios. Trate el desarrollo e implementación de software como un proceso de cambio. Integre las mejoras de seguridad en las actividades de gestión de cambios (p. ej., documentación y formación procedimental para usuarios y administradores).

10.3	*Datos de prueba*	Asegurar la protección de los datos usados para pruebas	Los datos utilizados para pruebas deben ser seleccionados cuidadosamente, protegidos y controlados	**Requerido**	Medición de porcentaje de datos utilizados en ambientes de desarrollo y que son utilizados en ambientes productivos basado en reportes de transacciones de aplicaciones realizadas en pruebas versus transacciones de aplicaciones realizadas en producción.	Incorpore una debida segregación de ambientes para asegurar que la información adecuada este siendo utilizada en el ambiente adecuado
11. Relaciones con los proveedores						
11.1	*Seguridad de la información en las relaciones con los proveedores*	Asegurar la protección de los activos de la organización que son accesibles por los proveedores	Debe existir una política de seguridad de la información para la relación con los proveedores y se debe acordar la seguridad dentro de los acuerdos con proveedores	**Requerido**	Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y estimadas como seguras.	Haga inventario de conexiones de red y flujos de información significativos con terceras partes, evalúe sus riesgos y revise los controles de seguridad de información existentes aspecto a los requisitos. Considere exigir certificados en NTS ISO/IEC 27001:2013 a los partners más críticos, tales como outsourcing de TI, proveedores de servicios de seguridad TI, etc.
11.2	*Gestión del servicio de entrega del proveedor*	Mantener un nivel acordado de seguridad de la información y el servicio de entrega alineados con los acuerdos del proveedor	Debería existir un monitoreo y revisión de los servicios del proveedor, así como también, hacer una debida gestión de cambios en los servicios del proveedor	**Requerido**	Coste del tiempo de inactividad debido al incumplimiento de los acuerdos de nivel de servicio.Evaluación del rendimiento de proveedores incluyendo la calidad de servicio, entrega, coste, etc.	¿Lo que recibe vale lo que paga por ello? Dé respuesta a esta pregunta y respáldela con hechos, estableciendo un sistema desupervisión de terceros proveedores de servicios y sus respectivas entregas de servicio. Revise periódicamente los acuerdos de nivel de servicio (SLA) y compárelos con los registros de supervisión.Esté atento a cambios que tengan impacto enla seguridad.
12. Gestión de incidentes de la seguridad de la información						

12.1	*Gestión de incidentes de seguridad de la información y mejoras*	Asegurar un enfoque consistente y efectivo para la gestión de incidentes de seguridad de la información, incluyendo la comunicación en los eventos y debilidades de seguridad	Se deben establecer procedimientos y responsabilidades de gestión para asegurar una respuesta rápida, al igual, que se debería informar sobre eventos y debilidades de seguridad de la información, para que posteriormente se pueda realizar una evaluación y toma de decisión del trato de los mismos. Debe existir una respuesta de incidentes de seguridad y aprendizaje de los mismos.	**Recomendable**	Número y gravedad de incidentes; evaluaciones de los costes de analizar, detener y reparar los incidentes y cualquier pérdida tangible o intangible producida. Porcentaje de incidentes de seguridad que han causado costes por encima de umbrales aceptables definidos por la dirección. Estadísticas del helpdesk de TI, con análisis sobre el número y tipos de llamadas relativas a seguridad de la información (p. ej., cambios de contraseña; porcentaje de preguntas acerca de riesgos y controles de seguridad de la información respecto al total de preguntas). A partir de las estadísticas, cree y publique una tabla de clasificación por departamentos (ajustada según el número de empleados por departamento), mostrando aquellos que están claramente concienciados con la seguridad, frente a los que no lo están.	Las revisiones post-incidentes y los casos de estudio para incidentes serios, tales como fraudes, ilustran los puntos débiles de control, identifican oportunidades de mejora y conforman por sí mismos un mecanismo eficaz de concientización en seguridad. Establezca y dé a conocer un punto único de llamadas (generalmente, el helpdesk habitual de TI) para que la gente pueda informar de incidentes, eventos y problemas de seguridad.
13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio						
13.1	*Continuidad de la seguridad de la información*	Incluir la continuidad de la seguridad de la información dentro de la gestión de la continuidad del negocio de la organización	Debe existir una planeación, implementación, verificación y revisión de la continuidad de la seguridad de la información	**Requerido**	Porcentaje de planes de continuidad de negocio en cada una de las fases del ciclo de vida (requerido / especificado / elaborado / probado). Porcentaje de unidades organizativas con planes de continuidad de negocio que han sido adecuadamente elaborados y probados mediante test apropiados en los últimos 12 meses.	Considere la gestión de continuidad de negocio como un proceso con entradas procedentes de diversas funciones (alta dirección, TI, operaciones, RRHH, etc.) y actividades (evaluación de riesgos, etc.). Asegure la coherencia y concientización mediante personas y unidades organizativas relevantes en los planes de continuidad de negocio. Deberían llevarse a cabo las pruebas pertinentes (tales como pruebas sobre el papel, simulacros, pruebas de failover, etc.) para mantener los planes actualizados, aumentar la confianza de la dirección en los planes y familiarizar a los empleados relevantes con sus funciones y responsabilidades bajo condiciones de desastre.

13.2	*Redundancias*	Asegurar la disponibilidad de las instalaciones de procesamiento de la información.	Lo que se busca es tener un escenario de alta disponibilidad para las instalaciones de procesamiento de la información.	**Recomendable**	Número de instalaciones y equipos disponibles para ofrecer redundancia en caso de un fallo	Considere poseer más de un sitio de contingencia, al menos, debe existir un sitio redundante ubicado en diferente ubicación geográfica para estar preparados ante cualquier desastre del sitio principal.
14. Cumplimiento						
14.1	*Cumplimiento con requerimientos legales y contractuales*	Evitar incumplimientos de las obligaciones legales, reglamentarias o contractuales relacionadas con la seguridad de la información y de cualquier requerimiento de seguridad	Realizar una identificación e implementación de la legislación aplicable, requerimientos contractuales, derechos de propiedad intelectual, protección de los registros, privacidad y protección de información identificada como personal, regulaciones de los controles criptográficos.	**Requerido**	Número de cuestiones o recomendaciones de cumplimiento legal, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de requisitos externos clave que, mediante auditorías objetivas o de otra forma admisible, han sido considerados conformes.	Obtenga asesoramiento legal competente, especialmente si la organización opera o tiene clientes en múltiples jurisdicciones.
14.2	*Revisiones de seguridad de la información*	Asegurar que la seguridad de la información se implemente y opere en concordancia con las políticas y procedimientos de la organización	Debe existir una revisión independiente de la seguridad de la información, así como también, del cumplimiento de las políticas, normas de seguridad y la parte técnica	**Requerido**	Número de cuestiones o recomendaciones de política interna y otros aspectos de cumplimiento, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de revisiones de cumplimiento de seguridad de la información sin incumplimientos sustanciales.	Alinee los procesos de auto-evaluación de controles de seguridad con las auto-evaluaciones de gobierno corporativo, cumplimiento legal y regulador, etc., complementados por revisiones de la dirección y verificaciones externas de buen funcionamiento.

6. Mejora del SGSI

6.1 Mejora continua

La mejora continua es una actividad periódica para desarrollar la capacidad a la hora de cumplir los requisitos, es un factor fundamental para cualquier sistema de gestión.

Las herramientas para la mejora continua son las revisiones de la dirección, las auditorías, las acciones correctivas, preventivas y de mejora, la política, los objetivos y el análisis de eventos e incidentes de seguridad. Los resultados de éstas actividades son una inestimable fuente de información sobre cuáles son las vulnerabilidades de la empresa y sus procesos. Sabiendo esto es posible tomar acciones encaminadas a eliminarlas, haciendo que los procesos sean más eficientes y efectivos.

6.2 Acción correctiva

Es una tarea que se emprende para corregir una no conformidad significativa con cualquiera de los requisitos del sistema de gestión de seguridad de la información.

Esta herramienta debe utilizarse para identificar errores o fallas en los procesos y no para buscar culpables. De no hacerse de ésta manera, es muy probable que el personal no colabore en la detección de las verdaderas causas raíz de los problemas y en la búsqueda de las soluciones.

La empresa debe realizar las acciones necesarias para eliminar las causas de las no conformidades con los requisitos del SGSI, a fin de evitar que vuelvan a producirse. El procedimiento establecido para las acciones correctivas debe definir los requisitos para:

A) Identificar las no conformidades;
B) Determinar las causas de las no conformidades;
C) Evaluar las necesidades de adoptar acciones para asegurarse de que las no conformidades no vuelvan a producirse;
D) Determinar e implantar las acciones correctivas necesarias;
E) Registrar los resultados de las acciones realizadas;
F) Revisar las acciones correctivas realizadas

6.3 Acción preventiva

Se aplican para evitar la aparición de futuras no conformidades. Son acciones encaminadas a eliminar la causa de una posible no conformidad.

En una acción preventiva se determina la posible fuente de problemas con el objetivo de eliminarla. Se pretende con ello tener que solucionar problemas, puesto que es más eficaz y sencillo prevenirlos que solucionarlos.

La empresa debe identificar las acciones necesarias para eliminar las causas de las posibles no conformidades con los requisitos del SGSI, para evitar que éstas vuelvan a producirse. Las acciones preventivas adoptadas deben ser apropiadas en relación a los efectos de los problemas potenciales. El procedimiento establecido para las acciones preventivas debe definir los requisitos para:

a) Identificar las posibles no conformidades y sus causas;

b) Evaluar la necesidad de adoptar acciones para prevenir la ocurrencia de no conformidades;
c) Determinar e implementar las acciones preventivas necesarias;
d) Registrar los resultados de las acciones adoptadas;
e) Registrar las acciones preventivas adoptadas

La empresa debe identificar los cambios en los riesgos, así como los requisitos de las acciones preventivas, centrando la atención en los riesgos que hayan sufrido cambios significativos.

La prioridad de las acciones preventivas debe determinarse basándose en los resultados de la evaluación de riesgos.

6.4 No conformidad y acciones correctivas

Cuando una no conformidad ocurre, la organización debe:

a) Reaccionar a la incidencia y según aplique:
    - Tomar acción para controlarla y corregirla
    - Lidiar con las consecuencias
b) Evaluar la necesidad de acciones para eliminar las causas de la no conformidad, de tal forma que esta no sea recurrente o se de en otros lugares, a través de:
    a. Revisar la no conformidad
    b. Determinar las causas de la no conformidad
    c. Determinar si podrían ocurrir no conformidades similares
c) Implementar cualquier acción necesaria
d) Revisar la efectividad de cualquier acción correctiva tomada
e) Realizar cambios al sistema de gestión de seguridad de la información, de ser necesario

Las acciones correctivas deben de corresponder a los efectos de las no conformidades encontradas. La empresa debe conservar información documental como evidencia de:

a) La naturaleza de las no conformidades y cualesquiera sean las acciones subsecuentes tomadas
b) Los resultados de cualquier acción correctiva

La empresa debe continuamente mejorar la idoneidad, adecuación y efectividad del sistema de gestión de la información.

Anexo A

(Informativo)

Correspondencia entre NTS ISO/IEC 27001:2013 y esta norma

La tabla A.1 muestra la correspondencia entre NTS ISO/IEC 27001:2013 y esta norma

Esta Norma	Norma NTS ISO/IEC 27001:2013
0. Introducción	0. Introducción
1. Alcance	1. Objeto
2. Referencias Normativas	2. Referencias Normativas
3. Términos y definiciones	3. Términos y definiciones
4. Requisitos a cumplir	4. Contexto de la organización 4.1 Comprensión de la organización y su contexto 4.2 Comprensión de las necesidades y expectativas de las partes interesadas 4.3 Determinar el alcance del sistema de gestión de seguridad de la información 4.4 Sistema de gestión de seguridad de la información
5. Guía de implementación	5. Liderazgo
6. Métricas y mediciones	6. Planeación 6.1 Acciones para abordar riesgos y oportunidades 6.2 Objetivos de seguridad de la información y planeación para lograrlos
7. Mejora continua	7. Soporte 7.1 Recursos 7.2 Competencia 7.3 Conciencia 7.4 Comunicación 7.5 Información documental
	8. Operación 8.1 Planeación y control operacional 8.2 Evaluación del riesgo de seguridad de la información 8.3 Tratamiento del riesgo de seguridad de la información
	9. Evaluación del desempeño
	10. Mejora
	Anexo A (Normativo) Objetivos de control y controles de referencia

Tabla A.1 – Correspondencia entre NTS ISO/IEC 27001:2013 y esta norma

Índice de Tablas

Tabla 1. Las PYMES se están preocupando por su seguridad informática. 12
Tabla 2. Criterios de seguridad de la información según estudios realizados en el año 2010 por McAfee y Panda Security 13
Tabla 3. Modelos/metodologías de gestión de seguridad 29
Tabla 4. Clasificación de las MIPYMES en El Salvador 32
Tabla 5. Clasificación de las empresas en El Salvador y su porcentaje en el mercado 33
Tabla 6. Pregunta No. 1 36
Tabla 7. Pregunta No. 2 37
Tabla 8. Pregunta No. 3 37
Tabla 9. Pregunta No. 4 38
Tabla 10. Pregunta No. 5 39
Tabla 11. Pregunta No. 6 40
Tabla 12. Pregunta No. 7 41
Tabla 13. Pregunta No. 8 42
Tabla 14. Pregunta No. 9 43
Tabla 15. Pregunta No. 10 44
Tabla 16. Pregunta No. 11 45
Tabla 17. Pregunta No. 12 46
Tabla 18. Pregunta No. 13 47
Tabla 19. Pregunta No. 14 48
Tabla 20. Pregunta No. 15 49
Tabla 21. Pregunta No. 16 50
Tabla 22. Pregunta No. 17 51
Tabla 23. Pregunta No. 18 52
Tabla 24. Pregunta No. 19 53
Tabla 25. Pregunta No. 20 54
Tabla 26. Pregunta No. 21 55
Tabla 27. Pregunta No. 22 56
Tabla 28. Pregunta No. 23 57
Tabla 29. Pregunta No. 24 58
Tabla 30. Pregunta No. 25 59
Tabla 31. Pregunta No. 26 60
Tabla 32. Pregunta No. 27 61
Tabla 33. Pregunta No. 28 62
Tabla 34. Pregunta No. 29 63
Tabla 35. Pregunta No. 30 64
Tabla 36. Pregunta No. 31 65
Tabla 37. Pregunta No. 32 66
Tabla 38. Pregunta No. 33 67
Tabla 39. Pregunta No. 34 68
Tabla 40. Pregunta No. 35 69
Tabla 41. Pregunta No. 36 70
Tabla 42. Pregunta No. 37 71

Tabla 43. Pregunta No. 38 73
Tabla 44. Pregunta No. 39 74
Tabla 45. Pregunta No. 40 75
Tabla 46. Pregunta No. 41 76
Tabla 47. Pregunta No. 42 77
Tabla 48. Pregunta No. 43 78
Tabla 49. Pregunta No. 44 79
Tabla 50. Pregunta No. 45 80
Tabla 51. Pregunta No. 46 81
Tabla 52. Pregunta No. 47 82
Tabla 53. Pregunta No. 48 83
Tabla 54. Pregunta No. 49 84
Tabla 55. Pregunta No. 50 85
Tabla 56. Pregunta No. 51 85
Tabla 57. Pregunta No. 52 86
Tabla 58. Pregunta No. 53 87
Tabla 59. Pregunta No. 54 89
Tabla 60. Pregunta No. 55 90
Tabla 61. Pregunta No. 56 91
Tabla 62. Pregunta No. 57 92
Tabla 63. Pregunta No. 58 93
Tabla 64. Pregunta No. 59 94
Tabla 65. Pregunta No. 60 95
Tabla 66. Pregunta No. 61 96
Tabla 67. Pregunta No. 62 97
Tabla 68. Pregunta No. 63 98
Tabla 69. Pregunta No. 64 99
Tabla 70. Pregunta No. 65 101
Tabla 71. Pregunta No. 66 102
Tabla 72. Pregunta No. 67 103
Tabla 73. Pregunta No. 68 104
Tabla 74. Pregunta No. 69 105
Tabla 75. Pregunta No. 70 105
Tabla 76. Pregunta No. 71 106
Tabla 77. Pregunta No. 72 107
Tabla 78. Pregunta No. 73 109
Tabla 79. Pregunta No. 74 110
Tabla 80. Pregunta No. 75 111
Tabla 81. Pregunta No. 76 111
Tabla 82. Pregunta No. 77 112
Tabla 83. Pregunta No. 78 113
Tabla 84. Pregunta No. 79 114
Tabla 85. Pregunta No. 80 115
Tabla 86. Pregunta No. 81 116

Tabla 87. Pregunta No. 82 117
Tabla 88. Pregunta No. 83 118
Tabla 89. Pregunta No. 84 119
Tabla 90. Pregunta No. 85 120

Índice de figuras

Figura 1. Cultura de la Seguridad de la Información 7
Figura 2. Principios de COBIT 23
Figura 3. El objetivo de Gobierno: Creación de Valor 23
Figura 4. Gobierno y Gestión en COBIT 24
Figura 5. Modelo de referencia de procesos de COBIT 5. 26
Figura 6. Las siete fases de la implementación del ciclo de vida 27
Figura 7. Distribución de empresas en El Salvador 33

Índice de gráficos

Gráfico 1. Pregunta No. 1 36
Gráfico 2. Pregunta No. 2 37
Gráfico 3. Pregunta No. 8 38
Gráfico 4. Pregunta No. 4 39
Gráfico 5. Pregunta No. 5 40
Gráfico 6. Pregunta No. 6 41
Gráfico 7. Pregunta No. 7 42
Gráfico 8. Pregunta No. 8 43
Gráfico 9. Pregunta No. 9 44
Gráfico 10. Pregunta No. 10 45
Gráfico 11. Pregunta No. 11 46
Gráfico 12. Pregunta No. 12 47
Gráfico 13. Pregunta No. 13 48
Gráfico 14. Pregunta No. 14 49
Gráfico 15. Pregunta No. 15 50
Gráfico 16. Pregunta No. 16 51
Gráfico 17. Pregunta No. 17 52
Gráfico 18. Pregunta No. 18 53
Gráfico 19. Pregunta No. 16 54
Gráfico 20. Pregunta No. 20 55
Gráfico 21. Pregunta No. 21 56
Gráfico 22. Pregunta No. 22 57
Gráfico 23. Pregunta No. 23 58
Gráfico 24. Pregunta No. 24 59
Gráfico 25. Pregunta No. 25 60
Gráfico 26. Pregunta No. 26 61
Gráfico 27. Pregunta No. 27 62
Gráfico 28. Pregunta No. 28 63
Gráfico 29. Pregunta No. 29 64
Gráfico 30. Pregunta No. 30 65
Gráfico 31. Pregunta No. 31 66
Gráfico 32. Pregunta No. 32 67
Gráfico 33. Pregunta No. 33 68
Gráfico 34. Pregunta No. 34 69
Gráfico 35. Pregunta No. 35 70
Gráfico 36. Pregunta No. 36 71
Gráfico 37. Pregunta No. 37 72
Gráfico 38. Pregunta No. 38 73
Gráfico 39. Pregunta No. 39 74
Gráfico 40. Pregunta No. 40 75
Gráfico 41. Pregunta No. 41 76
Gráfico 42. Pregunta No. 42 77
Gráfico 43. Pregunta No. 43 78

Gráfico 44. Pregunta No. 44 79
Gráfico 45. Pregunta No. 45 80
Gráfico 46. Pregunta No. 46 81
Gráfico 47. Pregunta No.47 82
Gráfico 48. Pregunta No. 48 83
Gráfico 49. Pregunta No. 49 84
Gráfico 50. Pregunta No. 50 85
Gráfico 51. Pregunta No. 51 86
Gráfico 52. Pregunta No. 52 87
Gráfico 53. Pregunta No. 53 88
Gráfico 54. Pregunta No. 54 89
Gráfico 55. Pregunta No. 55 90
Gráfico 56. Pregunta No. 56 91
Gráfico 57. Pregunta No. 57 92
Gráfico 58. Pregunta No. 58 93
Gráfico 59. Pregunta No. 59 94
Gráfico 60. Pregunta No. 60 95
Gráfico 61. Pregunta No. 61 96
Gráfico 62. Pregunta No. 62 97
Gráfico 63. Pregunta No. 63 99
Gráfico 64. Pregunta No. 64 100
Gráfico 65. Pregunta No. 65 101
Gráfico 66. Pregunta No. 66 102
Gráfico 67. Pregunta No. 67 103
Gráfico 68. Pregunta No. 68 104
Gráfico 69. Pregunta No. 69 105
Gráfico 70. Pregunta No. 70 106
Gráfico 71. Pregunta No. 71 107
Gráfico 72. Pregunta No. 72 108
Gráfico 73. Pregunta No. 73 109
Gráfico 74. Pregunta No. 74 110
Gráfico 75. Pregunta No. 75 111
Gráfico 76. Pregunta No. 76 112
Gráfico 77. Pregunta No. 77 113
Gráfico 78. Pregunta No. 78 114
Gráfico 79. Pregunta No. 79 115
Gráfico 80. Pregunta No. 80 116
Gráfico 81. Pregunta No. 81 117
Gráfico 82. Pregunta No. 82 118
Gráfico 83. Pregunta No. 83 119
Gráfico 84. Pregunta No. 84 120
Gráfico 85. Pregunta No. 85 121

Bibliografía

Comunicación, I. N. (Septiembre de 2012). *Estudio sobre seguridad de la información y continuidad de negocio en las pymes españolas.* Obtenido de https://www.incibe.es/file/Sp61c9ljOlMT7jcjbxYNVQ

Econocom. (http://itilv3.osiatis.es/). *ITIL FOUNDATION Gestión de Servicios TI*.

Estrada, A. C. (2011). *Seguridad por niveles.* Madrid.

Excellence, I. (11 de Abril de 2014). *SGSI Blog especializado en Sistemas de Gestión* . Obtenido de http://www.pmg-ssi.com/

Gobierno de España. Ministerio de Industria, E. y. (2014). *Instituto Nacional de Ciberseguridad*. Obtenido de https://www.incibe.es

INTECO. (Enero de 2010). *INTECO impulsa la implantación de SGSI en la PYME.* Obtenido de http://www.revistadintel.es/Revista/Numeros/Numero4/Seguridad/inteco.pdf

ISACA. (2012). COBIT 5 Un marco de negocio para el gobierno y la gestión de las TI de la Empresa.

ISO. (s.f.). Obtenido de https://www.iso.org

Luís Enrique Sánchez, D. V.-M. (s.f.). *MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES.* Obtenido de http://www.fing.edu.uy/inco/eventos/cibsi09/docs/Papers/CIBSI-Dia2-Sesion3(3).pdf

Normalización, O. S. (24 de Marzo de 2015). *www.osn.gob.sv*. Obtenido de http://www.osn.gob.sv/index.php?option=com_k2&view=item&id=113:osn-realiza-evento-de-difusi%C3%B3n-de-normas-en-tecnolog%C3%ADa-de-la-informaci%C3%B3n&Itemid=79

Observador, E. (31 de Marzo de 2015). *Seguridad de la información: un desafío para las pymes*. Obtenido de http://www.elobservador.com.uy/seguridad-la-informacion-un-desafio-las-pymes-n301687

S.L, L. (2014). *El blog de la gestión documental*. Obtenido de http://www.custodia-documental.com/familia-iso-27000-seguridad-de-la-informacion/

Standardization, I. O. (2012). *ISO27001.es*. Obtenido de http://www.iso27000.es/iso27000.html

Universidad Francisco Gavidia, E. S. (s.f.). *Publicación Bimensual de SCSI.* Obtenido de http://ri.ufg.edu.sv/jspui/bitstream/11592/7439/2/658.022-L735p-CAPITULO%20I.pdf