SEGURIDAD DE LA INFORMACIÓN EN EMPRESAS DE SERVICIOS PROFESIONALES

TRABAJO DE INVESTIGACIÓN FINAL

AUTORAS:

NATALIA VIRGINIA JUNCOS

EVELYN NOELIA VERA

TUTORA: MONICA REGINA DE ARTECHE

Resumen y Palabras Clave

En la actualidad, la información es usada como un recurso estratégico fundamental para las organizaciones que operan a nivel mundial. Es por ello que las mismas buscan constantemente la forma de proteger su activo más preciado de los posibles riesgos informáticos que rodean a las organizaciones.

Las empresas de servicios profesionales son empresas que se encargan de brindar diversos servicios como asesoramiento, auditoria, Consultoría y Outsourcing a terceros. Sin embargo, este servicio necesita, para poder cumplir con el objetivo propuesto, acceder a información clave de las organizaciones para las que va a trabajar.

Debido a eso, las empresas de servicios profesionales tienen desarrollado un gran sistema de seguridad de la información para proteger la información de terceros, sabiendo que si existe una fuga de datos por más mínima que sea expondrá a la empresa a las más severas consecuencias.

En este trabajo se buscó analizar la importancia de la seguridad de la información en las empresas de servicios profesionales especialmente en el grupo de las Big four. Para ello analizamos los distintos roles que tiene la información en las empresas, las reglamentaciones que proponen las normas ISO y cómo estás son aplicadas y entendidas por el personal.

Esta investigación ha demostrado la importancia y la sensibilidad que tienen los sistemas que implementan las empresas para proteger la información y como estas llevan un papel fundamental en las actividades que realizan los empleados en todo momento. A su vez, destacó la comunicación que existe entre los especialistas de seguridad informática con los gerentes de equipos y los empleados.

Palabras Clave: Información; Recursos estratégicos; empresas de servicios profesionales, seguridad de la información, seguridad informática.

Summary and Key Words

Nowadays, information is used as a fundamental strategic resource for Global organizations. This is the main reason why they search constantly the way to protect their most valuable asset from the possible IT risks that surrounds them.

Professional Services companies are companies that provide different kind of services as assurance, advisory, outsourcing, tax and legal. However, to reach the proposed objectives, this service needs access to key information in the organizations they are working with (the customers).

That is why Professional Services companies have developed an important Security Information System to protect the information from third parties, knowing that a minimum data leakage can expose the company to the most severe consequences.

In this investigation we analyzed the importance of Security Information in Professional Services Companies, especially in the group of the denominated Big Four. To do this, we analyzed the different roles that information has in companies, the regulation proposed by ISO rules, and the way they are applied and understood by the personnel.

This investigation has proved the importance and sensitiveness that the systems implemented in these companies have to protect the information and how they have an important role in the activities the personnel does all the time. Beside this, we emphasized the connection between the IT specialists with the team managers and personnel in general.

Key Words: Information; Strategic Resources; Professional Services Companies, Security Information.

1. Justificación

1.1 Problema

Las empresas de servicios profesionales se caracterizan por trabajar con un gran volumen de información de clientes que en la mayoría de los casos es confidencial para terceros. Con el desarrollo de las nuevas herramientas informáticas, el mayor uso de canales digitales para envío y transmisión de datos y las consecuencias que puede tener el mal manejo de esa información estas empresas se encuentran expuestas a diversos factores internos y externos que pueden perjudicar a la empresa prestadora del servicio y al cliente.

Debido a estos factores, muchas empresas se han visto perjudicadas, tanto en lo económico (representado por la pérdida de clientes por el mal uso de la información del mismo) como en lo legal y hasta penal (dependiendo de la gravedad del hecho involucrado, por ejemplo en empresas litigiosas cuya información es muy sensible), esto a su vez ha afectado la imagen de la alta dirección y ha hecho que organizaciones caracterizadas por su gran eficiencia se hayan visto arruinadas por esta clase de hechos.

En la actualidad, las empresas están destinando una gran cantidad recursos y esfuerzos para asegurar una mayor seguridad de la información con la que trabajan. Son un claro ejemplo de los mismos los distintos cursos y capacitaciones que se brindan al personal que trabaja en la organización, e-learnings, software que se aplica en los equipos informáticos, así como otras medidas técnicas (uso de passwords, firewall, etc.) y un conjunto de políticas implementadas que abarcan todos los aspectos en los que la seguridad de la información puede verse afectada. En el caso de las empresas de servicios profesionales más formalizadas, puede llegar a existir un documento que contiene la política aplicable a cada año fiscal.

Sin embargo, los riesgos en materia de seguridad de la información han evolucionado y continúan incrementándose cada vez más. Según la Encuesta Global de Seguridad de la Información (Global State of Information Security Survey)

preparada por la empresa PwC en colaboración con las revistas CIO Magazine y CSO Magazine, las empresas en la actualidad no han adoptado estrategias que acompañen el crecimiento de los riesgos, razón por la cual continúan aplicando políticas que no están preparadas para hacer frente a las amenazas actuales.

Con lo anteriormente expuesto y teniendo en cuenta que el objetivo de las empresas de servicios profesionales en este aspecto es proteger la información de sus clientes de todos los riesgos posibles que puedan surgir del mal uso de la misma, en este trabajo de investigación se hará un análisis de las medidas de protección en seguridad de la información llevadas a cabo por estas empresas, así como de los recursos empleados en estas medidas, y el grado de cumplimiento, conocimiento y entendimiento que obtienen estas políticas en las empresas.

1.2 Preguntas

- ¿Cuáles son las medidas llevadas a cabo por las empresas de servicios profesionales para la protección de la información de sus clientes?
- ¿En qué grado se entienden y se cumplen estas medidas?
- ¿Es posible lograr un mayor grado de cumplimiento?

1.3 Objetivos específicos

- Describir las medidas de seguridad implementadas por las empresas de servicios profesionales para la protección de la información de sus clientes.
- Determinar si las medidas actuales son acertadas o si es necesario aplicar nuevas.
- Identificar el alcance de las medidas implementadas y los recursos utilizados para su comunicación al usuario.
- Evaluar el cumplimiento de las medidas implementadas.

1.4 Hipótesis

Si bien las empresas destinan una gran cantidad de recursos para lograr el conocimiento, entendimiento y cumplimiento de las medidas de seguridad que se aplican para proteger la información, en muchos casos no es suficiente ya que el plan armado por el management muchas veces no logra ser lo suficientemente claro o comunicado de la mejor manera para lograr que los empleados cumplan con lo que se le solicita.

1.5 Alcance

Nos basaremos en analizar dos empresas líderes en el rubro de servicios profesionales que forman parte del grupo denominado Big Four tomando como objeto de análisis la firma miembro de Argentina. No se tomaran en cuenta el proceso en otros países, dado que estos procesos se encuentran estandarizados en la Red global de estas empresas.

2. Marco teórico

2.1 Capítulo 1- Empresas de servicios profesionales

2.1.1 Información en las Empresas de Servicios Profesionales

En el mundo actual, en el que las tecnologías cambian constantemente y es más fácil acceder a la información, a las empresas de servicios profesionales les resulta importante proteger la información por diversos motivos. El autor Idalberto Chiavenato (2006), analizando el concepto de información, expresa:

> Es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones (p. 11)

Los autores Collazo y Saroka (2010) apuntan su postura sobre este tema, afirmando que:

> La base de la riqueza es la información. La información genera la creación de conocimiento, que a su vez genera rápidas acciones estratégicas que crean ventajas competitivas, tanto sostenibles como temporarias. Más de la mitad de la fuerza de trabajo está involucrada en la recolección, el procesamiento y la comunicación de información (p. 110)

El principal motivo es que la información es un recurso que brinda poder y aquellas personas que tengan mayor acceso a la información podrán incidir en las decisiones que se tomen o anticiparse a alguna acción que los que la administran lleven a cabo. Esto proporcionara una ventaja competitiva sobre la empresa de la que fue filtrada la información y en muchos casos estas fugas no son detectables hasta que es

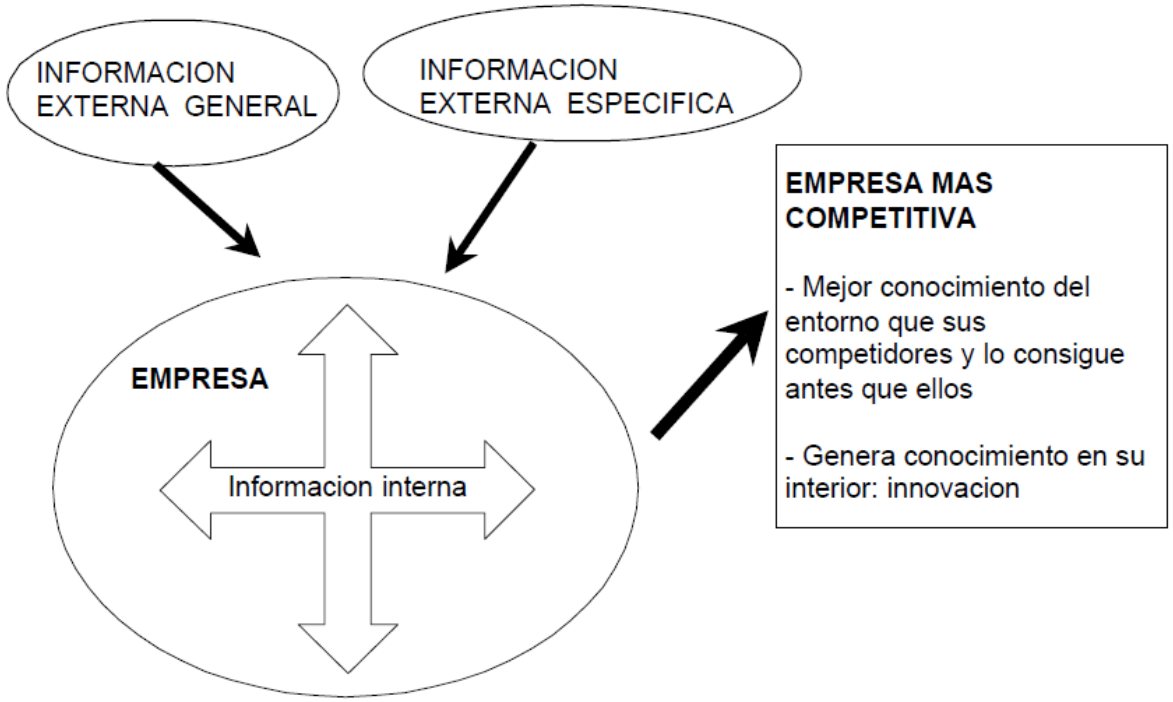
demasiado tarde. Otro motivo esencial en muchas empresas es que invertir en la protección de la información permite evitar pérdidas financieras provocadas por daños en bases de datos, desaparición de archivos, etc.

Los autores Porter y Miller (1986) analizan las posibilidades que utilizando la información de cada actividad de forma más eficiente se podrá lograr una mejora en la competitividad de las empresas. Mientras que Stalk (1988) caracteriza que la ventaja competitiva no se basa solo en el buen uso de la información sino hacerlo antes de que los competidores lo hagan.

Según un artículo escrito por la Facultad de Documentación, Universidad de Alcalá (1998), en el mismo se expresa que:

> El despliegue de sistemas informáticos y tecnologías para la comunicación, así como el desarrollo de las llamadas autopistas de la información ha generado un nuevo concepto: el de recurso informativo, cuyo valor trasciende el ámbito de las unidades de la información. En la actualidad se alude como recurso fundamental de cualquier tipo de organización o empresa. Se habla de él haciendo referencia a la ventaja competitiva de las empresas, y es obligada su mención cuando se trata de analizar los recursos que entran en juego en el desarrollo de una organización. La información se ha convertido, pues, en un bien económico, consideración de especial relevancia en la sociedad posindustrial […].

Figura 1: la informacion como recurso competitivo



Fuente: Antonio Paños Álvarez (1999)

En la imagen ilustrada arriba se observa como la empresa utiliza información externa e interna y que el buen uso de la misma generara una empresa más competitiva.

Según la autora Montuschi (2000), “Información son los datos que tienen “valor” y que el valor informativo depende del contexto.” A partir de esta frase se puede apreciar el valor subjetivo que se le puede dar a la información dependiendo de quien la maneje. A su vez, y siguiendo a otros autores, también agrega que “los datos se transforman en información cuando son interpretados por quien los recibe[…]”. Es por esto que se considera la importancia de hablar del tema de Seguridad de la Información: la información es un activo intangible invaluable para las empresas hoy en día, y más aún para las que trabajan con ella como recurso principal en su operatoria, como son las Empresas de Servicios Profesionales, explicadas con mayor detalle en el siguiente punto de este capítulo.

Las características más importantes que se intentan resguardar de la información son las siguientes:

- Confidencialidad: asegura que la información importante no se pone a disposición ni se provee acceso de ningún tipo a terceras partes (individuos, entidades o procesos) no autorizadas.
- Integridad: asegura que se mantiene la exactitud y completitud de la información y los métodos en los cuales la misma es procesada y manejada por los que tienen acceso a ella.
- Disponibilidad: se asegura que la información estará disponible para su acceso y utilización, así como de los sistemas de tratamiento de la misma de los terceros (individuos, entidades o procesos) autorizados cuando estos los requieran.

La brigada de Investigación tecnológica, su obra "Trabajo de Seguridad y protección de la información" establece a su vez otros aspectos importantes de la información:

Autenticidad: Permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar de quien dice ser.
Consistencia: Asegurar que el sistema se comporta como se supone que debe hacerlo con los usuarios autorizados.
Aislamiento: Regular el acceso al sistema, impidiendo que personas no autorizadas entre él.
Auditoria: Capacidad de determinar qué acciones o procesos se han llevado a cabo en el sistema, y quién y cuándo las han llevado a cabo.

Es decir que, la seguridad de la información es importante en una empresa, ya que la misma está destinada a garantizar estas tres características. Protege a la información de terceros no autorizados, que podrían darle un uso indebido como fue mencionado al comienzo del capítulo (el valor "subjetivo" de la información), como así también de los daños que la misma pueda sufrir, y que pueda provocar que no esté

disponible lo que conllevaría a pérdidas económicas, junto con la confianza del cliente.

La información con la que se trabaja se puede clasificar según su valor. Esta clasificación seria gerencial, operacional, documental, histórica. La información gerencial se caracteriza por ser aquella que le permite a la alta gerencia tomar decisiones que guiaran el rumbo de la empresa a largo plazo. Esta información es sumamente relevante en los aspectos de que si se divulga mucho de los aspectos intrínsecos de la empresa se conocerán y generaran perdidas incalculables.

Otra de las clases de la información es la operacional que se caracteriza por ser guías en las que se detallan los pasos para llevar a cabo distintos procesos. Ejemplo: compra de materia prima, elaboración de un producto, reportar un accidente, etc.

Dos clases más de información son aquellas que especifican un hecho en el pasado. Esta puede ser documental o histórica. La información documental se caracteriza por tener plasmados hechos que sucedieron en la empresa como pueden ser reportes anteriores, informes presentados a un superior, facturas de compra y recibos.

La última clasificación es la información histórica que permite ver cuáles eran las medidas tomadas en un sector hace un año con los resultados obtenidos y permite compararlos con las decisiones tomadas en la actualidad y sus resultados. Este tipo de información sirve principalmente para hacer comparaciones con años anteriores.

En el artículo titulado “Administración de la Información” publicado por la Universidad Centro Occidental, Lisandro Alvarado clasifica primero la información en dos grandes tipos de entorno inmediato y remoto. Para este trabajo nos enfocaremos en la información de entorno inmediato que se clasifica en las siguientes sub categorías:

- […]Clientes: El objetivo de esta información es mostrar las características, propiedades, las ventajas y las condiciones de adquisición de los productos o servicio prestado por la empresa. Toda empresa debe mantener informado a

sus posibles clientes sobre sus productos o servicios ya que sin comunicación con el cliente nunca van a existir posibilidades de negocio.

- Proveedores y distribuidores: Referida a información acerca de pedido, entrega, factura, devoluciones. A los distribuidores también se le enseña a través de catálogos, convenciones y otros actos destinados a difundir los productos o servicios de la empresa.
- Financiadores o inversionista: Reciben información económica financiera de la empresa a través de estados financieros, memorias, resúmenes de ejercicios económicos.
- Reguladores: Debe cumplir con las obligaciones fiscales lo cual conlleva a enviar formularios con datos e información sobre resultados de la empresa, igualmente con una serie de obligaciones informativas orientadas a la generación de estadística.
- Accionistas: Reciben información económica financiera de la empresa a través de estados financieros, memorias, resúmenes de ejercicios económicos.
- Empleados: Reciben información económica financiera de la empresa a través de estados financieros, memorias, resúmenes de ejercicios económicos […].

2.1.2 Las Big Four y la información que manejan

Las empresas de servicios profesionales operan en una industria que provee funciones técnicas o específicas, tanto a consumidores finales, como a empresas, en este caso tienden a llamarse “Servicios empresariales”.

Las Big Four son las firmas más importantes del mundo que trabajan dentro de esta industria, y se caracterizan por brindar servicios empresariales con grandes estándares de calidad, cuentan con recursos humanos altamente calificados y manejan los costos más competitivos del mercado.

Actualmente, el grupo se encuentra conformado por las siguientes empresas:

- Deloitte
- Ernst & Young
- KPMG
- PWC

Estas empresas proveen los siguientes servicios:

- Consultoría
- Auditoria
- Asesoramiento legal
- Asesoramiento impositivo
- Outsourcing (Contabilidad, impuestos, sueldos)

Teniendo en cuenta la clase de servicios que estas empresas brindan, las mismas necesitan tener un acceso privilegiado a la información de sus clientes.

Cada una de las categorías de servicios nombradas anteriormente requiere el acceso a determinada información, documentos y procesos con diferente grado de confidencialidad según sea el caso:

- Consultoría: al ser un servicio que brinda asesoramiento y apoyo profesional, el acceso a la información se remite principalmente a diferentes procesos y políticas que lleva a cabo la empresa tales como controles internos, políticas de manejo de riesgo en distintos aspectos, acceso a los diferentes procesos operacionales y financieros con el fin de evaluar posibles mejoras, revisión de la cadena de abastecimiento y CRM, efectividad de sistemas y políticas de recursos humanos con el fin de proveer cursos in Company.
- Auditoria: para realizar las tareas que abarca este servicio se necesita acceso a aspectos contables y regulatorios, sistemas de control interno, información financiero-contable de la empresa, debilidades en los controles y en los sistemas de procesamiento, tratamientos contables de operaciones complejas, etc.

- Asesoramiento legal: al trabajar en el ámbito del derecho en distintos aspectos (Derecho empresarial, laboral y seguridad social, comercio internacional, etc.), se tiene acceso a diferentes tipos de documentación, principalmente contratos y otros documentos legales, cartas, etc.
- Asesoramiento impositivo: este servicio implica el acceso al planeamiento tributario, a la situación fiscal de la empresa, declaraciones juradas, documentación relacionada con transferencia de precios, entre otras.
- Outsourcing: ya que este servicio se refiere a la tercerización de distintas funciones como contabilidad, impuestos y sueldos, requiere el acceso total a la operatoria habitual de estas actividades y todo lo que la realización de las mismas conlleva.

2.1.3 Normas ISO/IEC en las Empresas de Servicios Profesionales

La perspectiva del problema planteado por la Seguridad de la Información, que en un principio se entendía comprendido dentro del departamento informático de una empresa, como un conjunto de medidas de orden lógico y físico tendientes a proteger los activos intangibles valiosos (Información, conocimiento, etc.), ha ido evolucionando a medida que se comprendía el papel importante que juega el derecho en esta temática. El mismo advierte acerca de las políticas más adecuadas para cada empresa, a partir de lo cual se convirtió en un aspecto clave en la Gestión de la Seguridad de la Información.

Según Arean Hernando Velasco Melo (2008), la trascendencia de la seguridad de la información en las organizaciones públicas o privadas radica en que:

- El volumen de información crece día a día (dentro de lo llamado “La Era de la Información”);
- la información es un intangible con un valor bastante apreciable en la economía actual, dadas las características de la misma;
- la información es una ventaja estratégica en el mercado, que la convierte en algo atractivo para la competencia, como elemento generador de riqueza, el cual lo

convierte en una de las entradas clave en sistemas como los de gestión del conocimiento;

- la frecuencia de los ataques a los activos de una organización es cada vez mayor, cualquiera que sea el medio al que se acuda, y
- no existe una cultura de seguridad en los usuarios de la información.

Teniendo en cuenta todos estos puntos, es aquí donde se empieza a plantear la necesidad de desarrollar e incorporar prácticas que tiendan a proteger la información. Y surge la relación entre las nuevas Tecnologías de la Información y el derecho informático.

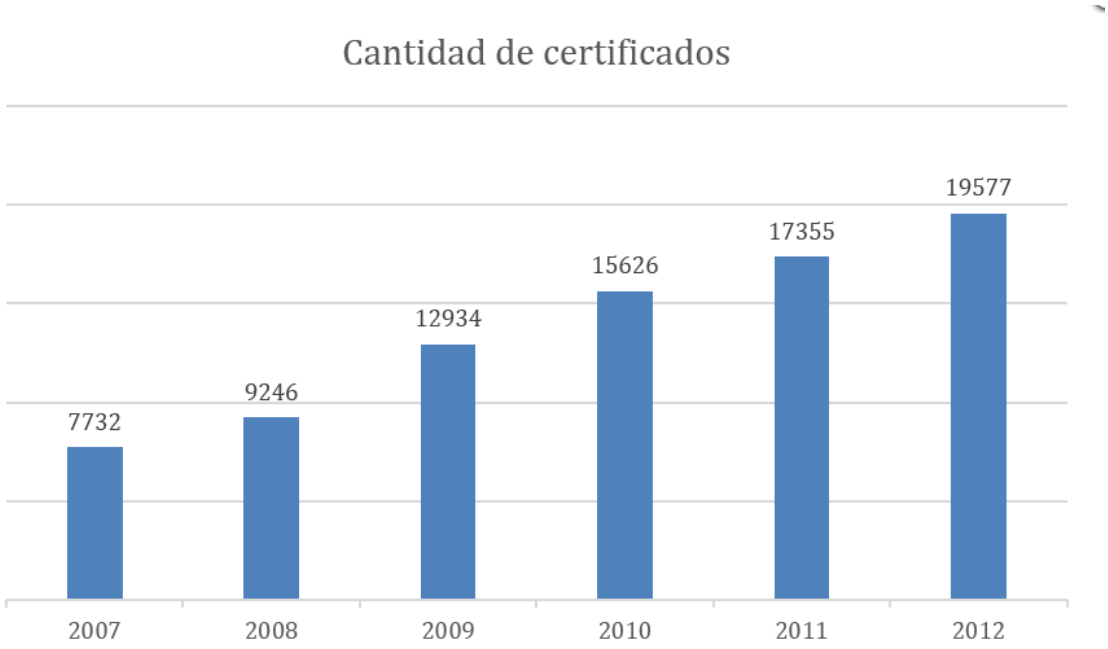
En este punto analizaremos el papel que le dedican las normas ISO a la seguridad de la información. La autora María Carme Sans (1998) define a la International Standarization Organization (ISO) como una la entidad internacional encargada de favorecer la normalización en el mundo. Con sede en Ginebra, es una federación de organismos nacionales, éstos, a su vez, son oficinas de normalización que actúan de delegadas en cada país, como por ejemplo: AENOR en España, AFNOR en Francia, DIN en Alemania, etc. con comités técnicos que llevan a término las normas. A su vez, define una norma como un modelo, un patrón, ejemplo o criterio a seguir. Una norma es una fórmula que tiene valor de regla y tiene por finalidad definir las características que debe poseer un objeto y los productos que han de tener una compatibilidad para ser usados a nivel internacional.

Según María Carme Sans (1998):

> La finalidad principal de las normas ISO es orientar, coordinar, simplificar y unificar los usos para conseguir menores costes y efectividad.
>
> Tiene valor indicativo y de guía. Actualmente su uso se va extendiendo y hay un gran interés en seguir las normas existentes porque desde el punto de vista económico reduce costes, tiempo y trabajo. Criterios de eficacia y de capacidad de respuesta a los cambios.

Es por esto que, al ser la seguridad de la información un proceso que se debe gestionar, se ha creado una norma que luego de varias actualizaciones se ha denominado ISO/IEC 27001. La misma es un estándar para la seguridad de la información emitida por la Organización Internacional de Normalización (ISO) e IEC (International Electrotechnical Commission) que describe como este aspecto debe ser gestionado en una empresa. Describe también su uso e implementación, y permite que una empresa sea certificada, es decir que mediante alguna entidad de certificación se puede asegurar que la misma cumple con la norma.

En los últimos años, al crecer la importancia del tema de Seguridad de la Información, la cantidad de empresas certificadas ha ido aumentando como lo muestra el siguiente gráfico:



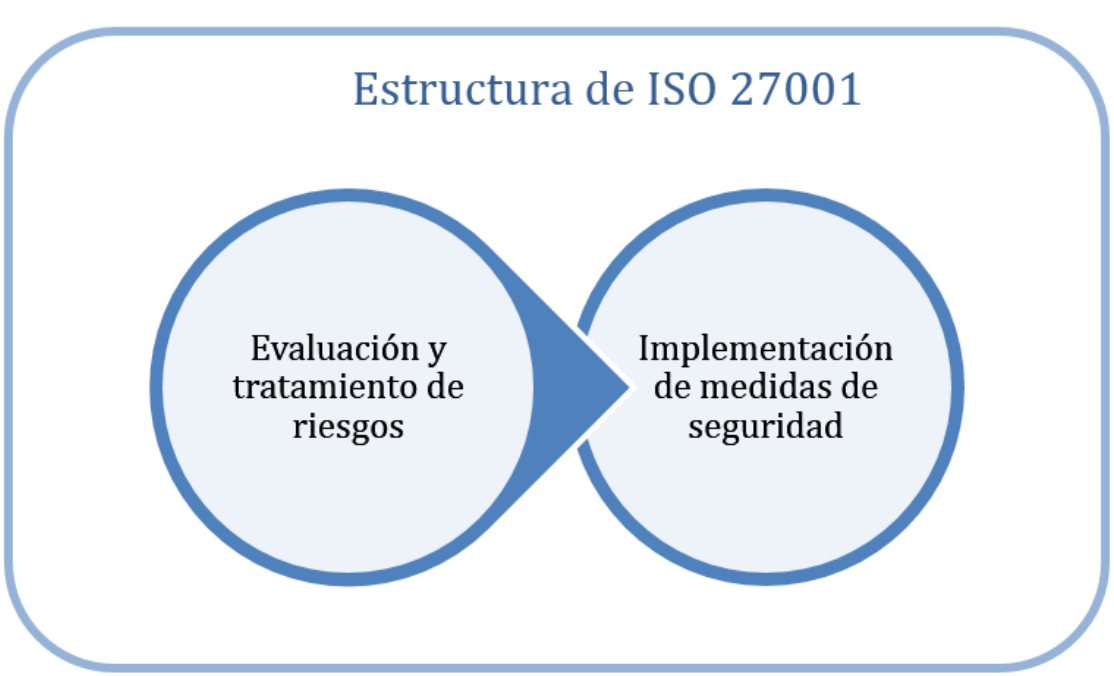
Fuente: Encuesta ISO sobre certificaciones de la norma para sistemas de gestión

La norma ISO/IEC 27001 sienta las bases para la creación de un Sistema de Gestión de la Seguridad de la Información (SGSI) que garantice la selección de controles y medidas adecuadas tendientes a la protección de los activos de una empresa y brinda confianza con respecto a los intereses de las partes que intervienen. En el caso de las Empresas de Servicios Profesionales, las partes

interesadas son la empresa misma y sus clientes. En otras palabras, esta norma garantiza a los clientes que su información está protegida.

El objetivo central de esta norma es proteger las características de la información en una empresa explicadas en el primer punto de este capítulo, las mismas son: confidencialidad, integridad y disponibilidad.

La estructura general del ISO/IEC 27001, al basarse en la gestión de riesgos, define las tareas que se realizaran, las mismas son: investigar acerca de los riesgos y los potenciales problemas que pueden afectar a la información, para luego tratarlos sistemáticamente, es decir definiendo lo necesario para evitar que los problemas se materialicen. Lo mencionado anteriormente se puede apreciar en el siguiente gráfico:



Fuente: "¿Cómo funciona la ISO 27001?"

El enfoque que propone la norma se fundamenta en normatividad nacional e internacional, y de otras fuentes del derecho, debido a la carencia de una legislación actual acerca del tema.

Propone un ciclo de seguridad en el que se contemplan diferentes dominios, que pretenden asegurar que el mismo sea lo más completo posible, los mismos son:

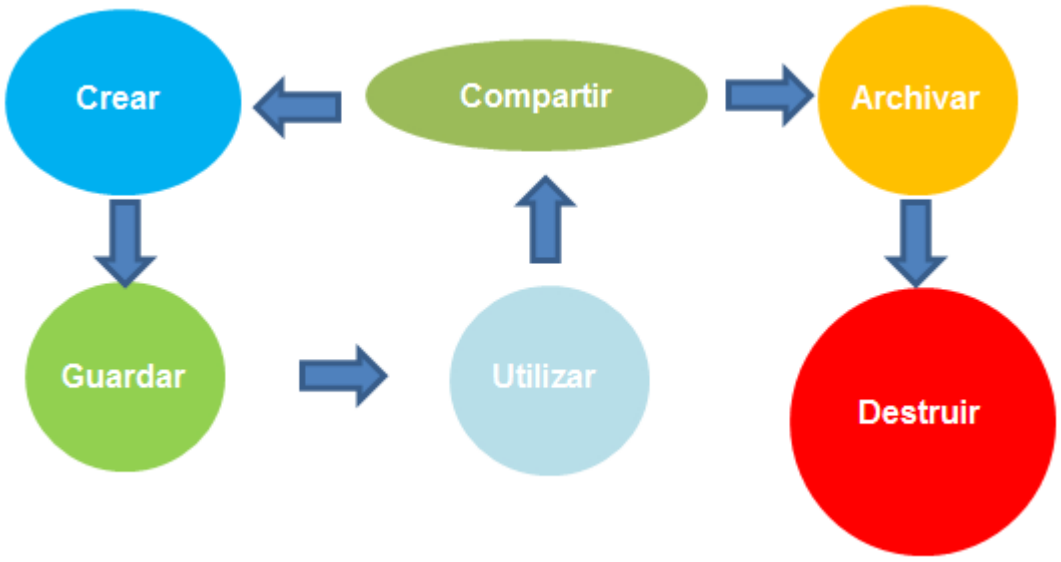
- Política de Seguridad de la Información
- Organización de la Seguridad de la Información
- Gestión de Activos
- Seguridad de los Recursos Humanos (Establecen los controles que deben tenerse en todos los momentos de la relación laboral, tanto antes, durante y después de la finalización de la contratación laboral).
- Seguridad Física y del Entorno
- Gestión de Comunicaciones y Operaciones
- Control de Acceso
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
- Gestión de Incidentes de la Seguridad de la Información
- Cumplimiento

Dentro de cada uno de estos dominios se plantean los diferentes controles que aseguren el cumplimiento del ciclo completo. Y teniendo en cuenta estos, se obtiene una perspectiva basada en procesos que hacen énfasis en la importancia de la comprensión de los requisitos de seguridad de la información, existencia de una política clara al respecto y los objetivos de la misma, existencia de controles, seguimiento y revisión y mejora continua.

Para resumir lo expuesto en el párrafo anterior, podemos citar al autor Arean Hernando Velasco Melo (2008): “Para el éxito de las recomendaciones jurídicas en materia de seguridad de la información es clave que las mismas estén alineadas con la estrategia y política general que la organización adopte en esta materia.”

Como anteriormente fue mencionado, la norma ISO 27001 sienta las bases sobre un concepto central conocido como Sistema de Gestión de Seguridad de la Información (SGSI, en ingles ISMS) el cual se constituye por un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo

empresarial. Este proceso resume el tratamiento que debe darse a la información y se puede observar en el siguiente gráfico:



Fuente: "¿Qué es un SGSI?", 2012.

Arean Hernando Velasco Melo (2008) describió lo siguiente:

> La comprensión de la finalidad y de los procesos involucrados en la aplicación de la norma ISO/IEC 27001 es un requisito fundamental para la adecuada contribución desde el Derecho al Sistema de Gestión de Seguridad de la Información en una organización[…].

Esto demuestra nuevamente que la implementación de un Sistema de Gestión de Seguridad de la Información dentro de las bases que sienta la norma ISO/IEC 27001 agrega al negocio la confianza que el Derecho Informático puede brindar al tema.

Los beneficios y ventajas que representan para la organización la implementación de un sistema de este tipo son los siguientes:

- Establece una metodología / política para la gestión de la seguridad, lo que puede contribuir a crear una cultura de control en la organización.

- Reduce ampliamente los riesgos relacionados con la información como la perdida, robo o corrupción de la misma.
- Los clientes mismos pueden corroborar el proceso debido a que tienen acceso a la información a través de medidas de seguridad.
- Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información. Revisión contínua de estos riesgos y sus controles.
- Crecimiento de la confianza de los clientes y socios estratégicos al garantizar la calidad y confidencialidad comercial y demostrar que la seguridad de su información es primordial.
- Implementación de auditorías externas que ayudan a identificar debilidades del sistema y áreas a mejorar del mismo.
- Posibilidad de integrarse con otros sistemas de gestión certificados como ISO 9001.
- Continuidad de las operaciones habituales del negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Diferenciación con otras empresas que no están certificadas, lo que brinda una imagen de empresa a nivel internacional.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costos y mejoras en los procesos.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.
- Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información.

A su vez, esta norma ISO/IEC 27001 forma parte de una serie de normas llamada “ISO/IEC 27000 series”, ya que como se mencionó anteriormente la misma solo sienta

las bases de cómo crear un SGSI y los requisitos que el mismo debe cumplir, pero no indica como cumplirlos. Para esto, se crearon las otras normas que forman parte de esta serie que van orientadas a completar las mejores prácticas, aspectos y cláusulas de modo que se eviten duplicar procesos y signifique un sustancial ahorro en el tiempo de implantación.

La serie está conformada por las siguientes normas, según el sitio web de la Norma ISO 27001 en Español:

- ISO/IEC 27000: 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 Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI.
- ISO/IEC 27001: Es la ya explicada anteriormente, la norma principal y la única certificable de la serie.
- ISO/IEC 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Contiene 39 objetivos de control y 133 controles.
- ISO/IEC 27003: Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI. 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.
- ISO/IEC 27004: 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.
- ISO/IEC 27005: Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma

ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

- ISO 27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Ayuda a interpretar los criterios de acreditación de ISO/IEC cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.
- ISO/IEC 27007: Es una guía de auditoría de un SGSI.
- ISO/IEC TR 27008: Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.
- ISO/IEC 27009: 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.
- ISO/IEC 27010: Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. La misma es aplicable a todas las formas de intercambio y difusión de información sensibles, tanto públicas como privadas, 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.
- ISO/IEC 27011: Es 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.
- ISO/IEC 27013: Principalmente es una guía de implementación integrada de ISO/IEC 27001.
- ISO/IEC 27014: Consiste en una guía de gobierno corporativo de la seguridad de la información.
- ISO/IEC TR 27015: Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros.
- ISO/IEC TR 27016: Consiste en una guía de valoración de los aspectos financieros de la seguridad de la información.

- ISO/IEC TS 27017: Consiste en una guía de seguridad para Cloud Computing.
- ISO/IEC 27018: Consiste en un código de buenas prácticas en controles de protección de datos para servicios de computación en Cloud Computing.
- ISO/IEC TR 27019: 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.
- ISO/IEC 27031: Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio.
- ISO/IEC 27032: 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, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP). Cubre las prácticas de seguridad a nivel básico para los interesados en el ciberespacio. Esta norma establece una descripción general de Seguridad Cibernética, una explicación de la relación entre la ciber-seguridad 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 ciber-seguridad.
- ISO/IEC 27033: Es una norma dedicada a la seguridad en redes.
- ISO/IEC 27034: Es una norma dedicada la seguridad en aplicaciones informáticas
- ISO/IEC 27035: Proporciona una guía sobre la gestión de incidentes de seguridad en la información.
- ISO/IEC 27036: Consiste en una guía en cuatro partes de seguridad en las relaciones con proveedores.
- ISO/IEC 27037: 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.

- ISO/IEC 27038: Consiste en una guía de especificación para seguridad en la redacción digital.
- ISO/IEC 27039: Consiste en una guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS).
- ISO/IEC 27040: Consiste en una guía para la seguridad en medios de almacenamiento.
- ISO/IEC 27041: Consiste en una guía para la garantizar la idoneidad y adecuación de los métodos de investigación.
- ISO/IEC 27042: Consiste en una guía con directrices para el análisis e interpretación de las evidencias digitales.
- ISO/IEC 27043: Desarrolla principios y procesos de investigación.
- ISO/IEC 27044: Sienta las bases para el desarrollo de la Gestión de eventos y de la seguridad de la información - Security Information and Event Management (SIEM).
- ISO 27799: Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002.

Cabe destacar que entre estas normas se encuentran algunas que ya han sido lanzadas, mientras que otras se encuentran en desarrollo. Pero todas ellas conforman una aproximación del Derecho Informático que existe sobre el tema.

2.2 Capítulo 2 – Vulnerabilidad ante la divulgación de la información

2.2.1 El riesgo de la divulgación de información en la actualidad

Las empresas lidian diariamente con distintos tipos de riesgos que puede afectar su trabajo cotidiano. Estos riesgos pueden ser económicos, tecnológicos, éticos, sociales, regulatorios y ambientales.

Los autores Ricardo Guagalango Vega y Patricio Moscoso Montalvo (2011) definen riesgo como estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Uno de los riesgos más importantes es el de la divulgación de la información, principalmente porque la información es el principal recurso de la empresa y su mal uso o que esté en manos de personas equivocadas puede causarle daños irreparables a la institución.

Podemos clarificar con la siguiente cita de las autoras Álvarez Zurita y García Guzmán (2007):

> Hay distintas fuentes las cuales pueden tener un impacto en la organización. Una fuente es llamada amenaza. Una amenaza tiene el potencial de causar un incidente no deseado, el cual puede provocar daños al sistema, la organización y a los activos. Pueden ser amenazas de la naturaleza, accidentes causados por negligencia o amenazas intencionales causadas por acciones maliciosas.

Hace unos años, las empresas solo debían preocuparse de la información que se encontraba en formato físico y era posible un mayor control debido a que esa información relevante solo se encontraba en un formato el cual solo accedía la persona que iba a trabajar con ella y después de su uso se destruía.

Sin embargo, con el surgimiento de nuevos dispositivos móviles de almacenamiento de información ha generado un nuevo riesgo especialmente porque

estos dispositivos son propiedad del empleado con el cual accede a la red de la empresa y descarga la información que necesita o porque se lleva información a su casa para poder terminar sus tareas fuera del horario de trabajo.

Podemos explicar lo anteriormente mencionado mediante la siguiente cita:

> La naturaleza y el tipo de tecnologías que constituyen la infraestructura de la información y comunicaciones también han cambiado de manera significativa. El número y tipo de dispositivos, servicios y variedades que integran la infraestructura de acceso se ha multiplicado, e incluye ya variados elementos de tecnología fija, inalámbrica y móvil, así como una proporción creciente de accesos que están conectados de manera permanente. Como consecuencia de todos estos cambios el volumen, naturaleza, disponibilidad y sensibilidad de la información que se intercambia a través de esta infraestructura se ha modificado y ha aumentado de manera muy significativa. (Voutssas, 2010).

El vicepresidente de ingeniería de GFI software, Simon Reed, comenta*:* "El 68% de las empresas se ponen en riesgo al subestimar la amenaza que supone para la seguridad de sus datos los dispositivos de almacenamiento" (2008).

A su vez, en muchos casos el empleado termina su relación laboral y continua manteniendo información confidencial y privilegiada y planea utilizarla en futuros empleos. En este caso, si se incurre en una divulgación de información es totalmente intencional ya que las personas que almacenan esta información o acceden fuera de su lugar de trabajo lo hacen con el único fin de poder terminar sus asignaciones y no tienen como objetivo que esta información sea pública o sacar algún beneficio por la divulgación de la misma.

Otro riesgo es que las personas que acceden a la información y hacen mal uso de ella. Estas personas lo único que tienen como objetivo es conseguir información que saben que es sensible y clave para las empresas y divulgarlas en distintos medios

para obtener un beneficio extra. Un ejemplo de este tipo de riesgo es el famoso caso de WikiLeaks que es un sitio web que divulgan información sensible de los gobiernos.

Otro de los riesgos que viene acompañado con la modernización es tener la información en el Cloud computing. Este tipo de almacenamiento de información les permite a los usuarios acceder a los archivos, informes y reportes que necesiten desde cualquier dispositivo móvil. Podemos definir el término Cloud Computing citando al autor Luis Joyanes (2009):

> Cloud computing es un conjunto de tecnologías de computación que están configurando un nuevo orden mundial en las TI que parte, esencialmente, de las expectativas creadas por la web 2.0 entre los usuarios personales y corporativos. [...] La idea clave es que los usuarios, las empresas, las grandes corporaciones acceden a los servicios de TI a través de la "nube" (cloud, una red pública, generalmente internet "la web" o una red intranet); los clientes pueden acceder bajo demanda - siguiendo el modelo "gratuito" o de "pago" por uso a un gran número de recursos informáticos de modo dinámico, tratándose así de una enorme capacidad de procesamiento y almacenamiento sin necesidad de instalar máquinas localmente, lo que se traduce en considerables ahorros de tiempo, e incluso de consumo energético.

Las principales ventajas de esta nuevo tipo de sistemas es que permiten tener toda la información en el mismo lugar y no ocupa espacio físico y está disponible las 24 horas del día los 365 días del año. A su vez para la empresa implica una reducción de costos operativos y administrativos y la inversión inicial termina siendo nula comparada con los resultado que da a largo plazo.

Entre las desventajas de tener la información en la nube se encuentra de que son servicios pocos personalizados ya que si bien cada empresa tiene su propia red no

tienen el sistema a medida del usuario sino que es un estándar para todos igual. Otra desventaja es el riesgo a la seguridad que generan ya que la información que se encuentra cargada en la nube puede ser adquirida por distintas personas a través de procesos fraudulentos y los mismos pueden divulgarla o modificarla.

Este riesgo viene también acompañado de que la información que se sube una vez en la nube es casi imposible poder borrarla por lo que las empresas deben ser sumamente criteriosas con la información que comparten con sus usuarios en las nubes y cuál debe ser compartida a un personal específico.

El ultimo riesgo más importante pero a su vez más identificable es el riesgo al ciberataque. El ciberataque es conocido como actos ilícitos que se basan en la intromisión de un agente totalmente externo al sistema en forma oculta para poder conseguir la mayor información posible y generar un daño irreparable. La realidad es que las empresas son conscientes de este riesgo pero no logran extinguirlos ya que es imposible a nivel organizacional seguir los cambios constantes de la tecnología.

2.2.2 Formas de mitigarlos

Los modelos de seguridad que se aplicaban en años anteriores ya no suelen ser eficaces dado que esos modelos se basaban en defender la información de amenazas externas. La realidad es que en la actualidad las amenazas pueden ser internas y externas.

Por eso, en la actualidad las empresas cuentan con planes de seguridad cuidadosamente planeados para prevenir todo tipo de amenazas tanto internas como externas y mantener la información confidencial resguardada de que sea de dominio público.

Las medidas tomadas para evitar amenazas externas son, entre una larga lista de acciones que pueden llevar a cabo, tendientes a proteger el acceso a los datos, quien puede tener acceso a los mismos, y protegerlos de terceros no autorizados.

Las políticas de seguridad son definidas por la autora Carolina Cols (nd.) como un conjunto de directrices, normas, procedimientos e instrucciones que guía las actuaciones de trabajo y define los criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como tecnológico.

Para la implementación de las políticas de seguridad la Universidad Nacional de Colombia define el siguiente esquema:

El ingeniero Leonardo Huertas Calle (2009) recomienda incluir los siguientes elementos al momento de implementar políticas de seguridad para los empleados:

- Alcance de las políticas, incluyendo facilidades, sistemas y personas sobre las cuales se le aplica.
- Objetivos de la política y descripción clara de los involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicados a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.

- Definición de violaciones y sanciones por no cumplir las políticas.
- Responsabilidades de los usuarios que tienen acceso a la información.

El Centro de Seguridad TIC de la Comunidad Valenciana (nd.) define 12 medidas básicas para la Seguridad Informática:

- Antivirus: Un antivirus es un programa informático específicamente diseñado para detectar y eliminar virus. Se debe programar para que revise la computadora de forma periódica.
- Instalar Firewalls que es un software destinado a garantizar la seguridad de las comunicaciones vía Internet al bloquear las entradas sin autorización a los ordenadores y restringir la salida de la información.
- Actualizar aplicaciones con “los parches de seguridad”: La mayoría de los software de gran difusión tienen la desventaja de ser el blanco de los hackers por lo que las empresas creadoras de los mismos lanzan al mercado con frecuencia los denominados parches de seguridad.
- Software legal: Ya que al instalar en los dispositivos de la organización software ilegales estos pueden ser vía de acceso para los Spyware.
- Precaución en la apertura de correo electrónico: Se debe tener sumo cuidado al abrir el correo electrónico y sospechar ante cualquier mail inesperado por más que sea de una persona conocida.
- Prudencia con los archivos: No se debe descargar de Internet ni de adjuntos de correos electrónicos, ni distribuya o abra ficheros ejecutables no solicitados y revise los mismos con el antivirus. A su vez, preste atención a quienes son las personas a las que se le envía dicha información.
- Administrador y usuario estándar: Diferencie la persona que administraran el sistema de aquellas que solo lo usaran en caso de que un usuario necesite ambos permisos se debe verificar que eso sea sumamente necesario. Ambos usuarios deben tener su acceso restringido a través de una contraseña.
- Contraseñas seguras: Se deben utilizar contraseñas distintas para accesos sumamente importantes y contraseñas similares para los accesos menos críticos.

- Navegación segura: Limite que los usuarios puedan acceder a páginas que puedan llegar a ser otra página de la que simula y sea una vía de acceso para los spyware,
- Copia segura: Se debe realizar de forma periódica copias de seguridad de la información más valiosa.
- Ayude a los demás: Cuando envié archivos a otras personas tenga la certeza de donde provienen los mismos ya que de dicha forma estaría enviándole a los demás empleados de la organización el riesgo que Ud. No detecto.
- Manténganse informado: Mantenga una constante actualización acerca de las medidas que se implementan en materia de seguridad.

Una de las medidas más importantes es crear un comité de seguridad que es definido por la autora Carolina Cols (nd.) como un equipo multidisciplinario que representa gran parte de la organización y que se reúnen periódicamente. Este comité es formado por un grupo definido de personas responsables por actividades referentes a la creación y aprobación de nuevas normas de seguridad en la organización.

2.2.3 Consecuencias de la divulgación de la información confidencial

Cuando una empresa de servicios profesionales firma con el cliente el contrato en el que se establece el servicio a brindar, el plazo, las partes intervinientes y demás condiciones, en el mismo se incluye la información que precisara cada una de las partes de la otra parte interviniente.

En la mayoría de los casos esta información es crucial y confidencial en el negocio de la empresa por lo que en el contrato se incluye un apartado que es un acuerdo de confidencialidad. Este acuerdo es una medida que tiene la empresa para protegerse del hecho de que una empresa totalmente ajena a su actividad haga mal uso de la información que accedió para realizar su trabajo y le genere inconvenientes legales y económicos en el futuro.

En este acuerdo de confidencialidad se encuentran distintas clausulas. La primera parte la empresa contratante del servicio se obliga a brindarle a la empresa prestadora toda la información que la misma necesite para llevar a cabo su tarea. Esta información se va a ir brindando a lo largo de que evolucione el proyecto que se lleve a cabo y solamente a las personas que deban hacer uso de la misma.

La cláusula que continua en el contrato es la de que por más que esta información sea brindada totalmente al momento de necesitarla, la propiedad de la misma siempre ve a ser de la empresa que brindo la información por lo que en ningún momento la empresa que recibió la información tendrá derechos sobre la misma e inclusive se puede llegar a establecer un plazo en él cual la empresa deba devolver toda la documentación que recibió.

Otra clausula también muy utilizada es que dicha información adquirida no podrá ser utilizada en proyectos futuros salvo autorización de la empresa que brindo la información. Una de las normas que se explicitan y más importante es la de la empresa que recibe la información se compromete a que todos sus empleados que accedan a dicha información van a hacer buen uso de la misma y respetaran todas las clausulas presentes en dicho contrato.

Si alguna de estas cláusulas no se cumplen existirán consecuencias diversas para las partes involucradas en el hecho. Una de las partes más afectadas va a ser la empresa que brindo su información confidencial y ahora la misma se encuentra en manos de personas que van a hacer mal uso de la misma o que la hicieron pública.

El hecho de que cierta información se publica permite conocer cómo son los procesos productivos al igual que administrativos y podrán imitarlos, como se encuentra la empresa a nivel contable y financiero por lo que podrán aprovecharse de esta situación al momento de negociar o incluso saber cuáles son sus estrategias en el futuro y la competencia podrá anticipar esos movimientos.

Estas pérdidas se cuantifican monetariamente para la empresa por ende la misma buscara un resarcimiento de parte de los culpables. Este resarcimiento primeramente va a ser económico y normalmente suele encontrarse establecido en la cláusula de

confidencialidad y en caso de que no se haya determinado, quedara a criterio del juez que se encargue de juzgar el hecho y en base a los daños provocados fijara la suma a pagar.

Otra sanción que determinara el juez será la sanción penal y económica para la persona que le brindo la información a un tercero o que hizo un uso impropio de la misma para un beneficio personal. La sanción estará determinada por el código penal basándose en la ley 26733 que dicta lo siguiente:

> […] Artículo 306: Será reprimido con prisión de uno (1) a cuatro (4) años, multa equivalente al monto de la operación, e inhabilitación especial de hasta cinco (5) años, el director, miembro de órgano de fiscalización, accionista, representante de accionista y todo el que por su trabajo, profesión o función dentro de una sociedad emisora, por sí o por persona interpuesta, suministrare o utilizare información privilegiada a la que hubiera tenido acceso en ocasión de su actividad, para la negociación, cotización, compra, venta o liquidación de valores negociables
>
> ARTICULO 5º -Incorpórese como artículo 308 del Código Penal de la Nación, el siguiente:
>
> Artículo 308:
>
> 1. Será reprimido con prisión de uno (1) a cuatro (4) años, multa equivalente al monto de la operación e inhabilitación de hasta cinco (5) años, el que:
>
> a) Realizare transacciones u operaciones que hicieren subir, mantener o bajar el precio de valores negociables u otros instrumentos financieros, valiéndose de noticias falsas, negociaciones fingidas, reunión o coalición entre los principales tenedores de la especie, con el fin de producir la apariencia de mayor liquidez

O de negociarla a un determinado precio;

b) Ofreciere valores negociables o instrumentos financieros, disimulando u ocultando hechos o circunstancias verdaderas o afirmando o haciendo entrever hechos o circunstancias falsas. […] (Ley 24733).

Esta sanción seria la básica pero se puede ver agravada si la persona genero peores consecuencias en el mercado de valores o genero perdidas irrecuperables para la empresa que expuso.

A su vez, como las personas que acceden a esta información son managers y se someten al código de ética del administrador de empresas primero deben cumplir con el siguiente deber: "[…] ARTICULO 11: Mantendrá el secreto profesional como norma de conducta de todas sus actuaciones realizadas con su ejercicio profesional, a no ser que haya autorización de las partes involucradas para divulgar información […]". (Ley 24733).

Y en caso de que no lo cumplan se verán expuestos a ser sancionados. Las sanciones que se les pueden aplicar se clasifican en leves o graves. Las sanciones pueden ser amonestación pública, amonestación privada, multas sucesivas, suspensión temporal de la matrícula, inhabilitación definitiva para ejercer la profesión.

La otra parte que también resultara perjudicada va a ser la empresa que tenía la información y no la pudo proteger. Las consecuencias para la empresa primero van a ser una sanción económica la cual afectara sus estados contables, además deberá costear todos los procesos judiciales si es sancionado en costas.

Sin embargo, la consecuencia que más perjudicara a la empresa va a ser que su imagen se dañara ante el mercado. Principalmente, porque todo este proceso judicial va ser difundido en los medios y también este caso va a ser tomado para que muchas empresas estudien en donde fallaron las medidas del Management para que no se vuelva a repetir. Además de que muchos clientes consideran que es peligroso que su información se encuentre en manos de una empresa que ya fue vulnerable ante los riesgos y preferirán contratar a otra empresa de servicios profesionales.

2.3 Capítulo 3 – Seguridad de la información en las empresas

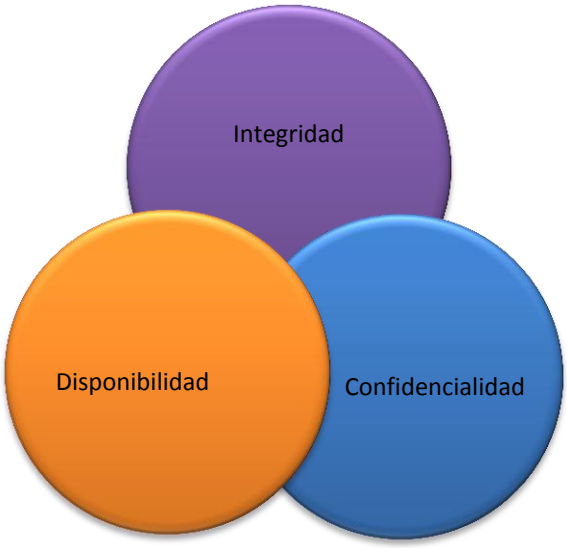
2.3.1 Implementación de la seguridad de la información en las empresas

Debido a los cambios que guiaron a la interconectividad y la interoperabilidad de las conexiones y el acceso simultaneo de la información por diversos ha generado que las empresas le empiecen a dar un lugar primordial a la seguridad dejando la misma de encargarse solo de proteger datos calificados por el gobierno como de acceso restringido.

En la actualidad, la seguridad de la información cumple un rol crucial en la empresa ya que esta permite defenderla de las amenazas externas e internas que pueden afectar a la organización y generarle pérdidas millonarias. Los objetivos principales de la seguridad de la información son preservar la confidencialidad de la información que se caracteriza para que solo esté disponible para aquellas personas que estén autorizadas a acceder a la misma.

Antonio Vaquero y Luis Joyanes (1993), definen la seguridad de la información como todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad y la integridad de la misma.

El otro objetivo es la integridad, sino que se deben asegurar de que esa información se encuentre en estado completo sin haber sufrido alteraciones por terceros y el último objetivo es su disponibilidad es que cualquier usuario que tenga permiso para poder acceder a dicha información de la forma y la manera que necesiten.



Fuente: Elaboración propia.

También existen otros objetivos generales de la seguridad de la información. Los mismos son conoce todos los riesgos de la empresa que se pueden prevenir con la seguridad, establecer requisitos de seguridad que sirva como filtro ante los riesgos, transformar las necesidades de seguridad en implementaciones que se lleven a cabo a diario, establecer la confianza de efectividad de los mecanismo de seguridad, determinar cuáles son los impactos operacionales que se deben llevar a cabo para disminuir los riesgos e integrar los esfuerzos del Management y del equipo técnico para que las estrategias sean llevadas a cabo.

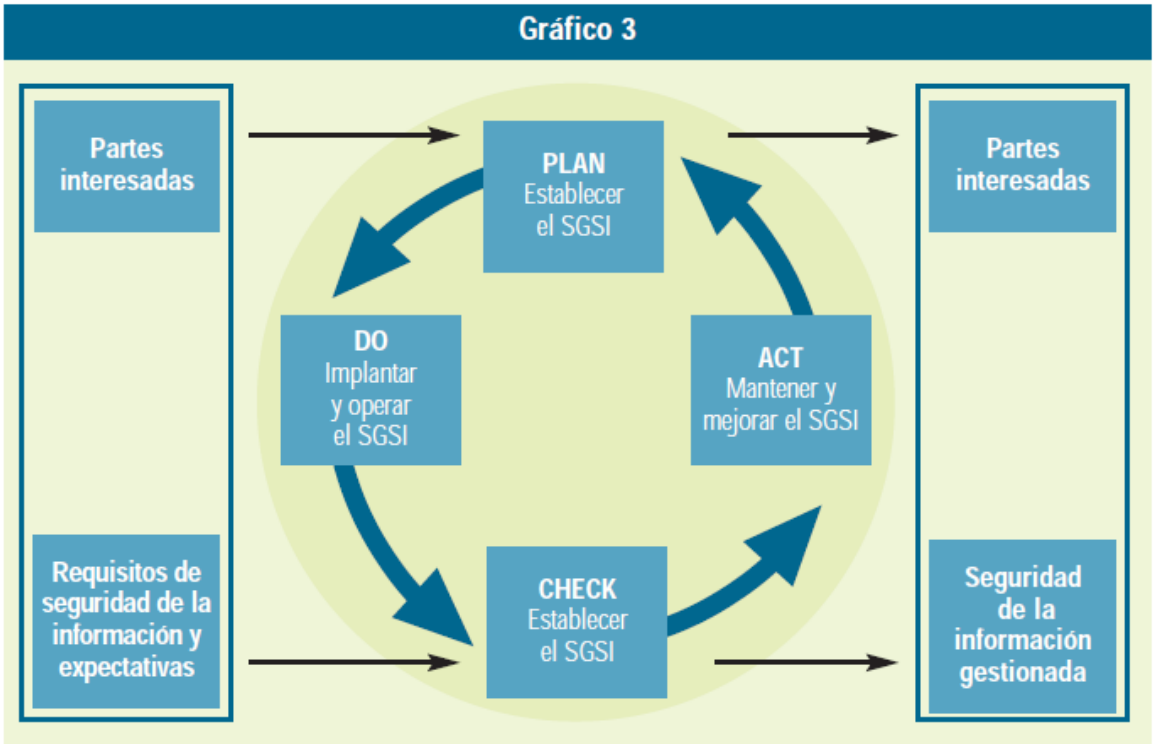
Cuando se piensa en adoptar un sistema de seguridad, las principales medidas que se piensan en adoptar son los estándares internacionales y por eso muchas veces se considera que las medidas de seguridad solo son útiles en las grandes empresas sin embargo estas medidas se pueden adaptar a distintas empresas sin importar el tamaño de la misma.

El jefe del grupo de seguridad lógica, Pablo Alonso (nd.), destaca seis aspectos básicos de la seguridad de la información:

- Principio del menor privilegio: cualquier objeto debe tener tan solo los privilegios de uso necesarios para desarrollar una tarea y ninguno más.

- Principio del eslabón débil: En todo sistema de seguridad, el máximo grado de seguridad no es la suma de toda la cadena de medidas sino el grado de seguridad de eslabón débil.
- Punto de control centralizado: Se trata de establecer un único punto de acceso a nuestro sistema, de modo que cualquier atacante que intente acceder, al mismo tenga que pasar por él. No se trata de utilizar un solo mecanismo de seguridad, sino de "alinearlos" todos de modo que el usuario tenga que pasar por ello para acceder al sistema.
- Seguridad en caso de fallo: Este principio afirma que en caso que cualquier mecanismo de seguridad falle, nuestro sistema debe quedar en estado seguro.
- Participación universal: Cualquier mecanismo de seguridad que establezcamos puede ser vulnerable si existe la participación voluntaria de algún usuario autorizado para romperlo.
- Simplicidad: Mantener las cosas lo más simple posible, las hace más fáciles de comprender mientras que la complejidad permite esconder múltiples fallos.

Al plantear un sistema de gestión de seguridad de la información se debe analizar cuáles son los activos que se deben resguardar y una vez identificados se debe lleva a cabo un modelo con cuatro niveles repetitivos. Los cuatro niveles son: planificar (PLAN), hacer (DO), verificar (CHECK) y actuar (ACT). La repetición constante de este ciclo genera una mejora continua en la seguridad.



Fuente: Ramón Robles & Álvaro Rodríguez de Roa (2006)

En la etapa de plan se analizan los riesgos, se crean las políticas de seguridad y se analiza su estado de aplicabilidad en la empresa considerando costos y beneficios. El siguiente paso será llevar a cabo las políticas antes analizadas y empezar a operar con el nuevo sistema de gestión de seguridad.

La tercer actividad es la de verificar si las políticas están teniendo los resultados esperados e ir auditando las distintas áreas en las que se están aplicando dichas políticas y comparar las estadísticas de la actualidad con el momento previo a la implementación del sistema. La última actividad se basa en hacer propuestas de mejoras y acciones correctivas para lograr un mejor resultado en la organización.

Según la empresa Ernst & Young un enfoque de seguridad integrado se debe basar en las siguientes etapas:

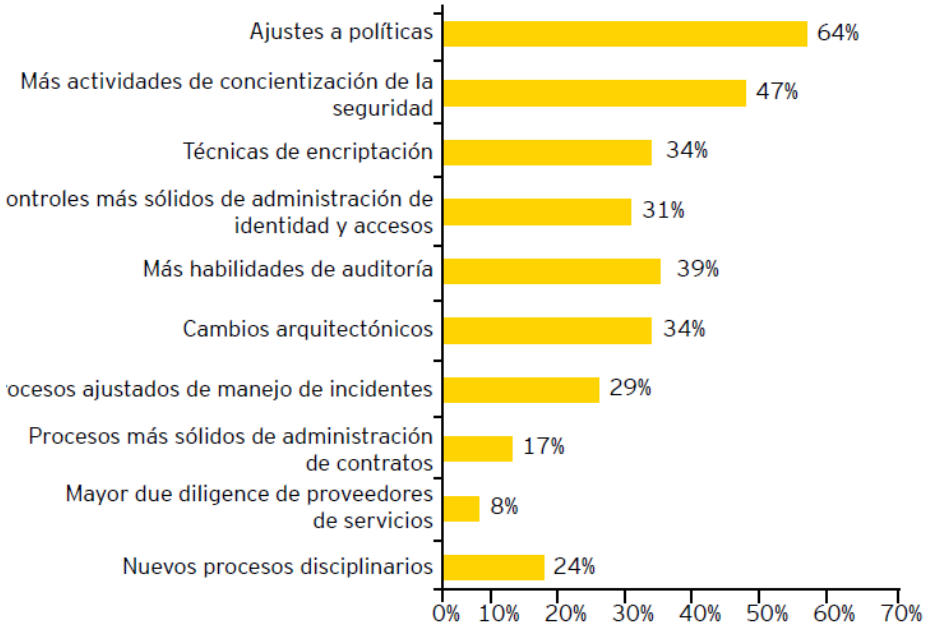
En primer lugar, identificar los riesgos reales, se debe analizar cuáles son los factores que ponen en riesgo a nuestra empresa ya sean interno o externo y ver de

qué manera se puede adelantarse a las amenazas ya que la mejor práctica de la seguridad es prevenir antes que corregir.

Para esta etapa es recomendable que se creen escenarios en los cuales se puedan analizar cuáles son las posibles amenazas que la información se encuentra expuesta no solo teniendo en cuenta el ámbito externo sino las personas que trabajan en la empresa.

El segundo paso se proteger lo importante, en esta etapa se plantea elaborar una estrategia que busque proteger la información que es considerada crucial y en entender que siempre la seguridad va a poder ser violada por lo que se debe buscar cómo mejorar los procesos y generar mejores condiciones para lograr que por más que hay una intromisión no puedan llegar a esta información.

La consultora se encargó de analiza cuales son las medidas que utilizan los gerentes para mejorar el resultado de las políticas de seguridad: los tres controles que más destacan son ajustar las políticas, más actividades de concientización de la seguridad y una mayor auditoria.



Muestra: porcentaje de encuestados
Fuente: *13a Encuesta Global de Seguridad de la información (EGSI) y comparativo México.*

La tercer etapa se basa en optimizar el desempeño para el negocio, lo que se busca es en optimizar y alinear todas las líneas de servicios con el objetivo de la línea de seguridad y a su vez en qué áreas invertir para que la seguridad sea plena.

Un aspecto en el que se hace hincapié es que las empresas cada día se destina una suma mayor del presupuesto al área de seguridad aunque no siempre es suficiente. Una manera para lograr que el presupuesto alcance seria tercerizar la parte más costosa y básica de la seguridad y de esa forma destinar todos los recursos en las actividades cruciales para lograr un mejor resultado.

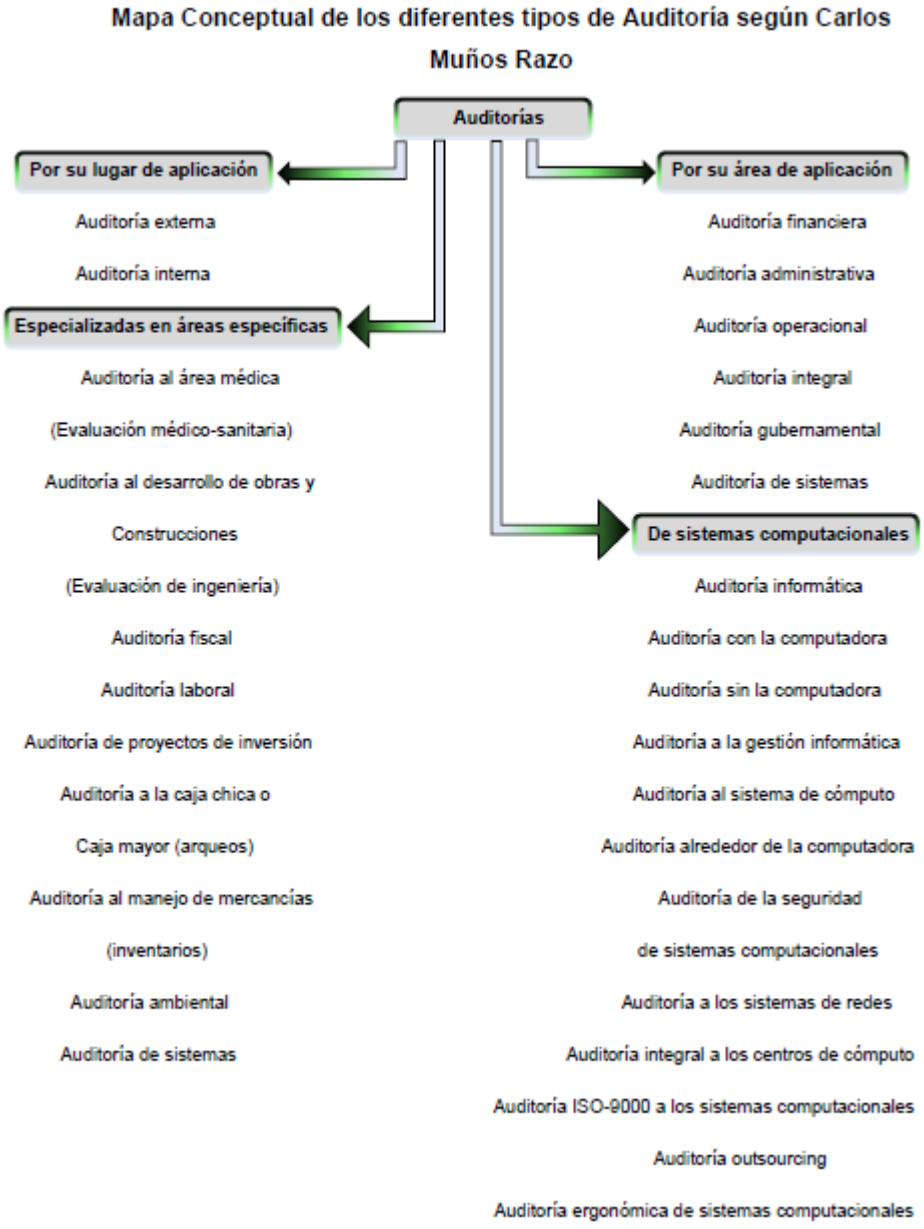
La última es ir más allá del cumplimiento de lo que se solicita sino lograr estar siempre en la vanguardia de lo que puede llegar a suceder y como prevenir estos daños en la empresa. El hecho de cumplir con lo que se solicita no implica que la empresa se encuentre protegida de cualquier amenaza. El departamento de seguridad de la información debe estar continuamente viendo cuales son las nuevas tendencias en materia de amenazas.

Los aspectos claves en los cuales se deben evaluar las medidas estratégicas de la información son: cantidad de amenazas reales, cantidad de archivos que se perdieron por ataque y cuando tiempo le lleva a la organización volver a su status quo después de un ataque.

En conclusión, si se desea que la implementación del sistema de seguridad sea un éxito se debe lograr que cada una de las personas de la organización entiendan que proteger la información debe ser un esfuerzo de todos y que si cada uno cumple con las directrices que se les dictan se obtendrá el resultado esperado. Caso contrario, si la empresa sufre una pérdida de información porque alguien no cumplió con lo solicitado toda la empresa resultara afectada.

A su vez, se debe entender que para tener un buen sistema de seguridad no es necesario restringir todos los dispositivos móviles sino que se debe buscar la manera de poder ingresarlos en la vida laboral pero tomando los recaudos necesarios para que no se conviertan en una amenaza a largo plazo

2.3.2 Auditoria de la Seguridad de la Información



En el grafico descripto anteriormente explica los distintos tipos posibles de auditoria y le da un gran espacio al desarrollo de la auditoria en los sistemas computacionales.

El autor Javier Moreno Bravo (2012) definió Auditoria informática como el conjunto de técnicas, procedimientos y actividades, destinados a analizar y evaluar el funcionamiento de los sistemas informáticos en un ente, por lo que comprende un examen metódico, puntual y discontinuo, con el propósito de mejorar aspectos como:

Control y seguridad de los sistemas informáticos, cumplimiento de la normativa tecnológica del ente, control de planes de contingencia, eficacia y rentabilidad en el manejo de sistemas.

En 1997, el autor Hernández Hernández definió a la auditoria en informática como un proceso formal orientado a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología con la que se maneja la información en una organización, se lleven a cabo de una manera oportuna y eficiente. A su vez, este proceso está compuesto por actividades ejecutadas por profesionales encaminadas a evaluar el grado de cumplimiento de políticas, controles y procedimientos correspondientes al uso de los recursos de informática e información por el personal de la empresa.

Entonces, teniendo en cuenta las definiciones descriptas en el párrafo anterior, la auditoria se basa en acciones tendientes al control y verificación. Mediante la misma, se corrobora que las políticas se estén llevando acorde a lo planeado y que las mismas se cumplan y cumplan con los objetivos de la gerencia.

Cabe destacar que existe cierta diferencia entre la auditoria informática y la auditoria de los sistemas de información. A continuación, desarrollaremos las similitudes y diferencias de las mismas a través de un cuadro desarrollado por el autor Javier Moreno Bravo.

Auditoria Informática y Auditoria de Sistemas de Información	
Similitudes	**Diferencias**
• No se requieren nuevas normas de auditoría, son las mismas.	• Se establecen algunos nuevos procedimientos de auditoría.
Los elementos básicos de un buen sistema de control contable interno siguen siendo los mismos; por ejemplo, la adecuada segregación de funciones.	• Hay diferencias en las técnicas destinadas a mantener un adecuado control interno contable.
• Los propósitos principales del estudio y la evaluación del control contable interno son la obtención de evidencia para respaldar una opinión y determinar la base, oportunidad y extensión de las pruebas futuras de auditoría.	• Hay alguna diferencia en la manera de estudiar y evaluar el control interno contable. • El énfasis en la evaluación de los sistemas manuales esta en la evaluación de transacciones, mientras que el énfasis en los sistemas informáticos, está en la evaluación del control interno.

Como ya fue mencionado anteriormente cuando se explicaron las normas ISO/IEC, hay 3 de ellas pertenecientes a la serie que sientan las bases de cómo debe realizarse la auditoria de los SGSI. Las mismas son explicadas mediante las normas ISO/IEC 27006, 27007 y 27008.

Según el sitio web ISO Tool, las bases para auditar las normas ISO 27001 se fundamentan en la norma ISO 27001:

- Gestión del programa de auditoria del SGSI: en el que establece qué, cuándo y cómo se debe auditar, gestionar los riesgos de auditoria, asignar auditores apropiados, mejora continua del proceso, mantenimiento de los registros de la misma.
- Realización de la auditoria relativa al SGSI: ésta incluye la planificación, el proceso de auditoría, la realización de actividades clave, análisis, trabajo de campo, presentación de informes y seguimiento. Gestión de los auditores del SGSI: competencias, habilidades, atributos, evaluación.

A su vez, tiene las siguientes finalidades:

- Corroborar la mitigación realizada por los controles de seguridad de la información de sobre los riesgos de la organización.
- Verificar que es correcta la relación de los controles de seguridad con la contabilidad general o de los sistemas y procesos de contratación para que los auditores verifiquen los datos.
- Comprobar que las obligaciones contractuales de los proveedores son satisfactorias. Realizar una revisión y control por la dirección.
- Operaciones rutinarias del SGSI de una organización para garantizar la buena marcha de la organización.
- Auditar después de producirse incidentes en la seguridad de la información como parte del análisis. Generar acciones correctivas.

2.4.3 Seguridad informática: De lo estratégico a lo táctico

Últimamente, podemos escuchar que se utilizan los términos seguridad informática y seguridad de la información como sinónimos. La realidad es que si bien ambos se basan en la protección de la información referente a las empresas, su diferencia se sitúa en que la seguridad de la información solo se enfoca en proteger toda la información de la organización sin importa en qué soporte se encuentra.

El autor Jean Marc Royer (2004) dice:

> El dominio cubierto por la seguridad informática es muy amplio. Esta se puede definir como la protección contra todos los daños sufridos o causados por la herramienta informática y originados por el acto voluntario y de mala fe de un empleado.

El principal objetivo de la seguridad de la información es el planeamiento de las estrategias que eviten que sucedan errores o actos deliberados del personal, ejecutan

un control sobre los cambios y emiten normas de comportamientos cuando existen vacíos legales.

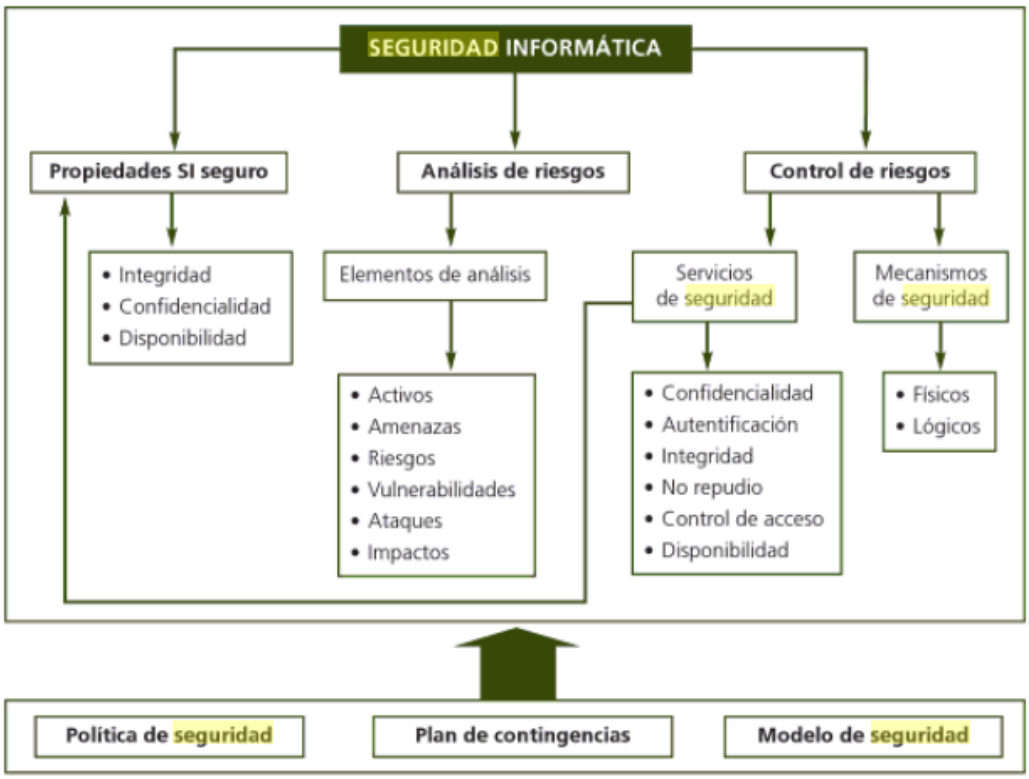
La eficacia de la seguridad de la información se mide evaluando la ganancia que produjo los cambios en materia de seguridad en la organización sobre la inversión realizada por la organización para llevar dichos cambios.

La seguridad informática se encarga de llevar a cabo la protección de estructuras tecnológicas y de comunicación que interactúan en una organización. A su vez su análisis de riesgo se basa en lograr que el riesgo de que se vulnere el hardware y software de la empresa sea mínimo y tolerable por la empresa.

Para establecer un sistema de seguridad informática, según el autor Purificación Aguilera López (2010) se determina que es necesario conocer:

- Cuáles son los elementos que componen el sistema.
- Cuáles son los peligros que afectan al sistema, accidentales o provocados.
- Cuáles son las medidas que deberían adoptarse para conocer, prevenir, impedir, reducir, o controlar los riesgos potenciales.

En conclusión, la seguridad informática se puede resumir de la siguiente manera según el autor Purificación Aguilera López (2010):

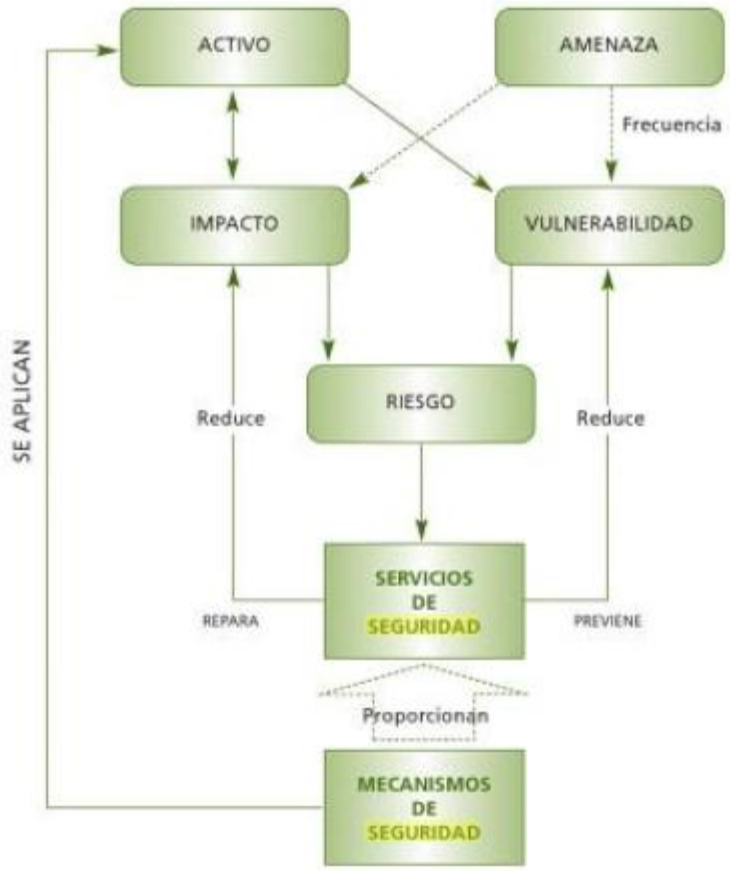


Las vulnerabilidades y amenazas en las que se enfoca la seguridad informática se suelen ser lógicas, físicas y humanas. Las amenazas físicas son robos, sabotajes, destrucción del sistema, robo de archivos y catástrofes naturales. El otro tipo son las humanas, en esta clase se consideran todas las personas ya sean empleados, ex – empleados, intrusos remunerados y hackers. La ultima amenaza son las lógicas que se conocen como virus, gusanos, caballos de Troya, software incorrecto y canales cubiertos.

Y las formas en las que pueden actuar se dividen en activas y pasivas. Las activas son aquellas que buscan evitar un ataque en el sistema por lo que ponen un filtrado en las conexiones, encriptan datos y la pasiva actúa una vez que ya ocurrió el daño y lo que busca es minimizar el mismo.

En resumen, seguridad de la información se encarga planificar y llevar a cabo las estrategias para minimizar los riesgos, asegurando la disponibilidad, confidencialidad e integridad de la información en cambio la seguridad informática lleva a cabo las

medidas tácticas para proteger la información. Y su circuito se puede definir de la siguiente forma según el autor Purificación Aguilera López (2010):



3. Metodología de la Investigación y Trabajo de Campo

3.1 Metodología de la investigación

Antes de realizar una investigación de campo, es necesario aplicar un diseño de investigación. Como explica el autor Malhotra (2007):

> Un diseño de investigación es un esquema o programa para llevar a cabo el proyecto de investigación[…]. Aunque ya se haya desarrollado un enfoque amplio del problema, el diseño de investigación especifica los detalles –los aspectos prácticos- de la implementación de dicho enfoque. Un diseño de la investigación establece las bases para realizar el proyecto. (p. 78).

Existen dos métodos de investigación: cualitativo y cuantitativo, los cuales se diferencian en distintos aspectos. Según el mismo autor se caracterizan de la siguiente manera: “La investigación cualitativa proporciona conocimientos y comprensión del entorno del problema; mientras que la investigación cuantitativa busca cuantificar los datos y por lo general, aplica algún tipo de análisis estadístico” (p. 143).

Para el autor Kuhn (1962), los términos métodos cualitativos y métodos cuantitativos significan mucho más que técnicas específicas para la recogida de datos. Resulta más adecuadamente una conceptualización de dos paradigmas, es decir un conjunto de suposiciones interrelacionadas respecto al mundo social que proporciona un marco filosófico para el estudio organizado del mundo.

A su vez, el autor Kuhn (1970) amplía la definición diciendo que representa una “matriz disciplinaria” que abarca generalizaciones, supuestos, valores, creencias y ejemplos corrientemente compartidos de lo que constituye el interés de una disciplina.

Según Blázquez Entonado (1988):

> El paradigma cuantitativo se atribuye a una visión del mercado positivista, hipotético-deductivo, particularista, objetivo, orientada hacia resultados y propia de la ciencia natural. En cambio, se dice que el paradigma cualitativo se adscribe a una visión del mundo fenomenológica, inductiva, holística, subjetiva, orientada hacia el proceso propio de la antropología social. (p. 38).

Grinnell (1997), citado por Hernández et al (2003:5) señala que los dos enfoques (cuantitativo y cualitativo) utilizan cinco fases similares y relacionadas entre sí:

a) Llevan a cabo observación y evaluación de fenómenos.

b) Establecen suposiciones o ideas como consecuencia de la observación y evaluación realizadas.

c) Prueban y demuestran el grado en que las suposiciones o ideas tienen fundamento.

d) Revisan tales suposiciones o ideas sobre la base de las pruebas o del análisis.

e) Proponen nuevas observaciones y evaluaciones para esclarecer, modificar, cimentar y/o fundamentar las suposiciones o ideas; o incluso para generar otras.

Teniendo en cuenta lo mencionado anteriormente, consideramos necesaria la utilización de los dos tipos de métodos para lograr una investigación eficaz y eficiente del proyecto de investigación. A partir de esto, el paradigma que vamos a aplicar en nuestra investigación es el cuali-cuantitativo ya que nos permitirá obtener una mejor visión de la seguridad de la información en las empresas de servicios profesionales, al lograr mediante el paradigma cualitativo un conocimiento y entendimiento del entorno y el problema, y mediante el paradigma cuantitativo una cuantificación de los datos obtenidos.

Los elementos que utilizaremos en nuestra investigación son los siguientes: entrevistas a especialistas en Seguridad de la información, entrevistas a gerentes funcionales que lideren equipos que manejan información sensible en una Empresa de Servicios Profesionales miembro de las Big Four y encuestas dirigidas a empleados de estos equipos.

La primera herramienta a utilizar son las entrevistas. Malhotra (2007), las define de esta manera:

> "[…] las entrevistas en profundidad son una forma no estructurada y directa de obtener información[…] dichas entrevistas se realizan de forma individualizada. Una entrevista en profundidad es una entrevista no estructurada, directa y personal en la que un entrevistador[…] interroga a una sola persona, con la finalidad de indagar sus motivaciones, creencias, actitudes y sentimientos subyacentes acerca de un tema. (p. 158).

Para llevarla a cabo se utiliza un cuestionario, en el que se plantean preguntas para el entrevistado. Sus ventajas principales son que permiten obtener un mayor control de las respuestas, ya que las mismas se atribuyen directamente al participante y producen un intercambio libre de información, a su vez también permiten indagar, según Malhotra (2007) "la indagación es sumamente importante para obtener respuestas con significado[…]" (p. 159).

Utilizaremos dos tipos de cuestionarios para nuestra investigación, uno por cada perfil entrevistado, los cuales caracterizaremos a continuación:

1) Especialistas en Seguridad de la información: El objetivo que perseguimos con esta herramienta es lograr obtener el procedimiento que conlleva la implementación de un sistema de seguridad de la información en grandes empresas. Analizar cuáles son las mejores prácticas que se deben llevar a cabo en la actividad diaria empresarial.

También buscamos ver si se aplican las normas ISO o si aplican otro tipo de medidas para la protección de la información y como son las mismas llevadas a cabo. Otro aspecto que también buscaremos indagar es como son auditadas y cuál es el sistema de control para evaluar el grado de implementación de estas medidas.

El perfil de los entrevistados será:

- Tener entre 30 y 50 años
- Ser gerentes o especialistas en departamentos que se encarguen de la seguridad de la información en las empresas
- Evalúen si las normas de seguridad son acordes a los acuerdos de confidencialidad en los cuales la empresa forma parte.

2) Gerentes Funcionales de una Big Four: El objetivo de esta herramienta metodológica será evaluar como la seguridad de las empresas afecta en la vida cotidiana y como ellos ayudan a sus empleados a que puedan cumplir con los requisitos que les establece la gerencia de seguridad de la información. Otra de los aspectos que se desean evaluar es los procedimientos que utilizan para proteger la información y como plan de acción definido que se debe llevar a cabo en el caso de que exista una fuga de información.

Otro de los objetivos es encontrar las medidas que se aplican para lograr que los empleados conozcan las normas de seguridad y como ellos motivan a que se interesen para que las conozcan.

El perfil de los entrevistados:

- Tener entre 30 y 50 años
- Ser gerentes o gerentes seniors en empresas de servicios profesionales.
- Deben tener más de un año como gerentes
- Apliquen normas de seguridad en sus empresas.
- Participen en negociaciones con otras empresas

- Deban liderar grupos que manejen información sensible de terceros

Por último, utilizaremos encuestas. Las mismas son un instrumento propio de la investigación cuantitativa, y para su análisis se pueden utilizar una serie de elementos estadísticos, como ser tablas o gráficos.

Según el autor Malhotra (2007), las encuestas se caracterizan de la siguiente manera:

> La técnica de encuesta para obtener información se basa en el interrogatorio de los individuos a quienes se les plantea una variedad de preguntas[…]. Estas preguntas se pueden hacer verbalmente, por escrito, mediante una computadora, y las respuestas se pueden obtener en cualquiera de estas formas. Por lo general, el interrogatorio es estructurado, lo cual se refiere al grado de estandarización impuesto por el proceso de recolección de datos. En la recolección estructurada de datos se prepara un cuestionario formal, y las preguntas se plantean en un orden predeterminado[…]. (p. 183).

Con las encuestas se busca poder obtener la perspectiva de los empleados que son una parte fundamental en el modelo de seguridad en las grandes empresas. A través de una serie de preguntas buscaremos ver como las empresas les comunican a los empleados prácticas que deben cumplir para proteger la información y cual son los procedimientos que ellos deben realizar, como así también el grado en que conocen y entienden las medidas que aplican y la valoración de la información y el riesgo que perciben.

Perfil de los encuestados:

Encuestaremos empleados con distintos rangos de edad y antigüedad, como así también que trabajen o hayan trabajado en distintos puestos de diversas jerarquías, y

en distintas áreas. Utilizaremos esta segmentación en el análisis de las encuestas, para evaluar distintos aspectos en el que cruzaremos las variables.

Con estos tres elementos mencionados en los párrafos anteriores, lograremos la triangulación en nuestra investigación.

3.2 Cuadro de Metodología

Variables	Dimensiones	Indicadores	Instrumento	Entrevista Especialista IT	Entrevista Gerente Funcional	Encuestas Usuarios
Mejores prácticas en seguridad de la Información	Normas ISO 27001	Implementación de las Normas ISO en empresas de servicios profesionales	Entrevista Especialista IT	Ítem 1		
		Formas de aplicación de los dominios		Ítem 2		
		Conocimiento y aplicación de las Normas ISO	Entrevista Gerente Funcional		Ítem 1	
	Formas de mitigar los riesgos	Mejores prácticas aplicadas	Entrevista Especialista IT	Ítem 3		
		Controles que aplican a su equipo para observar el cumplimiento de las normas y medidas	Entrevista Gerente Funcional		Ítem 2	
	Acuerdos de confidencialidad	Cambios que se deben hacer en el sistema de trabajo según el cliente con el que se trabaje	Entrevista Especialista IT	Ítem 4		
		Dificultad en la adaptación de las nuevas practicas	Entrevista Gerente Funcional		Ítem 3	
	Implementación de la seguridad de la información en empresas	Complejidad de llevar a cabo un SGSI	Entrevista Especialista IT	Ítem 5		
		Comunicación de las mejores prácticas a los grupos de trabajo	Entrevista Gerente Funcional		Ítem 4	
		Planes de capacitación	Entrevista Gerente Funcional		Ítem 4	
			Entrevista Especialista IT	Ítem 6		
			Encuestas Usuarios			Ítem 13
	Seguridad Informática	Medidas técnicas en una implementación de un SGSI	Entrevista Especialista IT	Ítem 7		
		Medidas técnicas que utilizan los empleados	Encuestas Usuarios			Ítem 8
		Conocimiento y aceptación de las normas por parte de los empleados				Ítem 12 - Ítem 14

Variables	Dimensiones	Indicadores	Instrumento	Entrevista Especialista IT	Entrevista Gerente Funcional	Encuestas Usuarios
Grado de implementación y cumplimiento	Importancia de la Información	Usos y acceso a la información	Encuestas Usuarios			Ítem 7
		Grado de importancia de la información				Ítem 6
		Características de la información en el trabajo diario	Entrevista Gerente Funcional		Ítem 5	
	Riesgo a la divulgación de la información	Conocimiento de las amenazas existentes	Encuestas Usuarios			Ítem 9
		Percepción de los riesgos posibles en la actividad diaria	Entrevista Gerente Funcional		Ítem 6	
		Formas de análisis de riesgos	Entrevista Especialista IT	Ítem 8		
		Plan de acción ante un incidente de seguridad	Entrevista Gerente Funcional		Ítem 7	
	Consecuencias del mal uso	Conocimiento de las consecuencias negativas	Encuestas Usuarios			Ítem 10
		Percepción del impacto de las acciones propias en la seguridad de la información				Ítem 11
		Medidas correctivas después de un incidente de seguridad	Entrevista Especialista IT	Ítem 9		
			Entrevista Gerente Funcional		Ítem 8	
	Auditoria en seguridad de la información	Características del proceso de auditoria	Entrevista Especialista IT	Ítem 10		
		Grado de control hacia los usuarios	Encuestas Usuarios			Ítem 15 - Ítem 16

3.3 Análisis de las entrevistas

3.3.1 Especialista IT de una Big Four

El día 27 de Octubre de 2014 se realizó una entrevista en las oficinas del IT Supervisor de una Big Four, Licenciado en Administración de la UBA con un MBA de la UCEMA. A lo largo de su carrera profesional se ha desempeñado en organizaciones tanto públicas como privadas en sectores afines a IT, sistemas y soporte técnico que lo llevan a definirse como un profesional en IT con experiencia en organizaciones con compleja infraestructura tecnológica. En su puesto actual sus tareas consisten en:

- Supervisión y coordinación de proyectos informáticos.
- Gerenciamiento de las Operaciones de IT
- Desarrollo de Business Continuity Plan de la Empresa en Argentina
- Se encuentra a cargo del equipo de Information Security de IT
- Implementación de Políticas de Seguridad de la Información y participación activa en las actividades del Comité de Seguridad y las Auditorias
- Supervisión de Soporte Técnico

En la entrevista se trataron diferentes cuestiones como la implementación y certificación de la Norma ISO 27001, complejidades y desafíos de un SGSI en una empresa de Servicios Profesionales, como así también se indago acerca del punto de nuestro mayor interés que es el impacto que tiene el tema de Seguridad de la Información para el management.

El especialista nos indicó que la implementación y certificación de la Norma ISO 27001 es muy importante ya que en ella están contenidas las mejores prácticas que debe adoptar una Empresa de Servicios Profesionales en lo que respecta a Seguridad de la Información. Para poder implementar esta norma, es necesario partir de una política, que según sus palabras es la “ley” en la empresa sobre este tema, y al ser bastante complejo su contenido, al usuario final le llega una información distinta, mas resumida y contenida en un “Manual de Seguridad de la Información” que está basado en esta política. Es decir que la misma rige los lineamientos en los que se van a basar

las medidas adoptadas, y las bases sobre las que se lleva a cabo el sistema de trabajo, el cual no puede ser cambiado por más que algún cliente tenga requerimientos especiales, si los mismos atentan contra la política de la empresa.

Entre otras cosas, también nos comentó que los dominios que forman parte de la norma, mencionados en el marco teórico, se aplican mediante una serie de controles que indican los requisitos que cada dominio debe cumplir, algunos de ellos con aplicaciones netamente técnicas.

En lo que respecta a la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), el entrevistado nos señaló las principales medidas técnicas que se llevan a cabo: sistemas de antivirus, securizacion perimetral de la red y manejo de vulnerabilidades. También nos comentó uno de los principales desafíos que se debe enfrentar con una implicancia directa en el Management en la implementación de un SGSI: encontrar un correcto equilibrio entre la creación de un entorno de seguridad aceptable para la empresa (con toda la inversión y esfuerzos que esto implica) y la rentabilidad del negocio, lo que representa un análisis de los puntos críticos en las operaciones para saber en cuales conviene invertir y cuál es el impacto de un posible riesgo. Para poder realizar este análisis y lograr este equilibrio, es importante tener en cuenta las características de la información con la que se trabaja: confidencialidad, integridad y disponibilidad.

En otra de las preguntas realizadas, el especialista profundiza en el mencionado análisis de riesgos y nos cuenta que hay que considerar una combinación de dos factores: probabilidad e impacto. Es en este punto en el que se lleva a cabo un Risk Assesment, que implica considerar que riesgos hay que mitigar, y que otros se pueden llegar a aceptar ya que no forman parte de un punto crítico del negocio. Esto se considera de alto impacto en el management, ya que al lograr una mayor seguridad conlleva a mayores costos, lo que podría afectar al “Business Continuity”.

En cuanto a las capacitaciones que se realizan a los empleados, el entrevistado nos indica que lo más importante es lograr una comunicación periódica de estos

temas, que se pueden dar por distintos medios, ya sea por e-learnings, e-mails, o capacitaciones presenciales.

En el caso que suceda algún incidente que implique fuga de información, existe un plan definido para evitar que el mismo vuelva a ocurrir, como primera medida se debe aislar el incidente para evitar que el mismo se propague y poder investigar las causas que lo llevaron a generarse. El paso siguiente, dependiendo del caso, puede ser la implementación de nuevos controles que refuercen las medidas adoptadas anteriormente.

Finalizando con la entrevista, al especialista se le consulto acerca del proceso de auditoría de un SGSI y nos mencionó que en este proceso se analizan los controles llevados a cabo y las evidencias sobre la realización de los mismos.

3.3.2 Gerente Funcional de una Big Four (1)

Una contadora que se desempeña como gerente de auditoria en una Big Four fue entrevistada el día 27 de octubre de 2014, para comentarnos desde su perspectiva como es el manejo de la Seguridad de la Información en grupos de trabajo en una empresa de Servicios Profesionales.

Se consultó con la entrevistada acerca de las medidas que llevan a cabo los empleados en el transcurso de las actividades diarias, algunas de ellas como encriptación de archivos, cables de seguridad en laptops, claves de acceso, entre otras. También afirmó que estas medidas son requeridas por la política de la casa matriz y que las mismas se comunican a los empleados en charlas periódicas para reforzar el mensaje. Con respecto a los controles que se llevan a cabo para asegurar las medidas anteriormente mencionadas, comenta que se deben modificar las claves de acceso y se monitorean los archivos.

La contadora nos comentó que en algunos casos, antes de comenzar a trabajar con algún nuevo cliente es necesario solicitar permisos especiales para acceder a su información y nos comenta que la misma, para la mayoría de los clientes, se trata de información restringida, con importancia alta ya que incide en la toma de decisiones.

Finalmente la entrevistada nos comenta que es fácil identificar los riesgos en la operatoria diaria, y que en la experiencia que tiene en su puesto nunca ha tenido conocimiento de algún incidente ocurrido, por lo cual no conoce acerca las acciones correctivas que se aplican para que el mismo no vuelva a ocurrir.

3.3.3 Directora de Operaciones de una Big Four

Realizamos una entrevista a la Directora de Operaciones de una Big Four en su oficina para que nos cuente acerca del tema de Seguridad de la Información desde un panorama global, y como se aplica el mismo a todos los equipos de trabajo en general, desde una perspectiva del management.

La directora nos comento acerca de las medidas que se llevan a cabo, que son requeridas por la política de la casa matriz, que a su vez está basada en la norma ISO 27001. Con respecto a los controles que se llevan a cabo para asegurar estas medidas, los mismos son controles tanto físicos como lógicos de accesos, utilización de passwords, control de los anti-virus y otros software para los cuales se generan reportes, encriptación de dispositivos móviles, etc. También nos menciona que al trabajar con algún nuevo cliente no se modifican las prácticas habituales, ya que en ningún caso se puede reducir el nivel de seguridad establecido.

La entrevistada nos señala que las mejores prácticas que se llevan a cabo se comunican a los empleados mediante un portal de intranet el cual contiene las políticas y procedimientos, que están a disposición de todos y otras comunicaciones que tienden a reforzar las medidas de seguridad existentes, como así también menciona la existencia de un curso de Seguridad de la Información, el cual tiene que ser tomado por el empleado como requisito previo para empezar a trabajar con información de clientes.

Teniendo en cuenta las características de la información con la que se trabaja: confidencialidad, integridad y disponibilidad, la directora nos dice que la identificación de los riesgos que pueden surgir ante un mal uso de la misma es simple pero que el verdadero desafío es mitigarlos, y ya que la principal fuente de riesgo es interna, existe un principio de confianza básica en el empleado.

Nos comenta acerca de la existencia de un plan de manejo de incidentes el cual consiste en un plan de escalamiento y comunicación, colección de evidencia y posterior remediación, con roles y responsabilidades definidas. Existe un Comité de Information Security y Data Protection cuyo objetivo es revisar, proponer y aprobar las políticas de seguridad de la información y protección de datos. Este comité periódicamente revisa el estado general de seguridad de la información, notifica al Comité de accionistas y directorio sobre los incidentes identificados en auditorías internas y externas. Asimismo, analiza los casos que podrían ser incidentes de seguridad de la información y toma decisiones al respecto. Por último promueve la concientización de la seguridad de la información en toda la organización.

Con respecto a acciones correctivas luego de un incidente, después de pasar por el mencionado plan de acción y comité, se revisan los controles para evitar que la fuga de información vuelva a ocurrir.

3.3.4 Gerente Funcional de una Big Four (2)

Entrevistamos a un Gerente Senior de una Big Four, licenciado en Administración de Empresas, con una antigüedad de más de 7 años en la empresa el día 5 de Noviembre de 2014. El mismo ha participado en distintos proyectos de consultoría y revisión de procesos en distintos clientes liderando grupos de trabajo que manejan información, también tiene experiencia en negociaciones para licitaciones de proyectos con diversos clientes donde la seguridad de la información fue un aspecto a analizar.

El entrevistado nos dio su punto de vista sobre las distintas preguntas en que lo interrogamos, en ellas se indago acerca de temas como las medidas que se llevan a cabo en una Big Four y los controles tendientes a asegurar el cumplimiento de las mismas, también como se comunican estas medidas a los grupos de trabajo.

Nos señaló el licenciado que lo principal en este tema son las Políticas definidas por el área de Seguridad de la Información de la empresa, y que en ellas están contenidas todas las medidas tendientes a proteger la información tanto propia como de los clientes. También nos menciona alguna de estas medidas que aplica su grupo

de trabajo, entre ellas las más importantes son control de los mails que se envían y repositorios online que actúan como una especie de base de datos que define los permisos y accesos que tiene cada empleado a determinado tipo de información. Estas medidas mencionadas podrían modificarse o incluso agregarse nuevas, en caso de que algún cliente lo solicite. También con respecto al tratamiento de la información que se transmite vía email, nos señala que lo importante es tratar de concientizar a los empleados, ya que en última instancia las acciones de los mismos dependen de la conciencia y moral de cada uno, dejando implícito un principio de confianza en el empleado. Otro punto a destacar, es que el entrevistado desconoce acerca de los estándares internacionales en los que se basan las políticas implementadas por el management.

Las medidas y políticas llevadas a cabo son comunicadas a los grupos de trabajo vía email, principalmente para reforzar y recordar a los empleados el cumplimiento de las mismas, y aunque es poco común la realización de capacitaciones presenciales, también se realizan cursos online bajo la modalidad e-learning.

Con respecto a las características de la información, el entrevistado comenta que la misma es crítica, confidencial y altamente sensible. También nos comenta que los riesgos que pueden surgir ante un mal manejo de la información siempre son los mismos, lo que cambia es el impacto que tienen según el tamaño del cliente con el que se esté trabajando. Hace una distinción en lo que respecta a proyectos en los que trabajan muchas personas, en este caso la identificación de los riesgos y el control sobre los mismos se vuelve más difícil.

Nos señala el licenciado que desconoce si dentro de las políticas implementadas existe algún plan de acción definido ante un incidente de seguridad, valiéndose únicamente de su criterio profesional en el caso de que fuera necesario. Teniendo en cuenta esto, como acciones correctivas considera una posibilidad alguna mejora en los sistemas o revisión de los procesos y controles.

3.3.5 Especialista en Seguridad de la Información certificado en ISO

El 23 de octubre de 2014 entrevistamos a un Ingeniero en Computación, certificado en ISO 27001 que cuenta con una amplia experiencia realizando actividades como la implementación de estándares y mejores prácticas de seguridad, coordinación del Sistema de Gestión de Seguridad de la Información y auditorías de seguridad informática.

El ingeniero nos comento acerca de los procedimientos que intervienen en la implementación de la norma ISO 27001, es decir en la implementación de un SGSI. Como punto de partida resulta importante contar con el apoyo de la alta dirección. Una vez que se cuenta con esto, hay que tener bien en claro las necesidades y expectativas de las partes, como así también el alcance del SGSI. Finalmente se define la política de seguridad, conjuntamente como los métodos de análisis de riesgos y tratamiento de los mismos (planes de acción definidos) y auditorias.

Con respecto a los dominios de la norma, el entrevistado afirma que se implementan mediante controles técnicos de seguridad que suelen incluirse en documentos llamados Declaración de Aplicabilidad y se generan después de haber realizado una evaluación de los riesgos. Nos comenta también, que esta evaluación de riesgos puede tomar como base a la norma ISO 27005, combinada con algún otro método que aplique al negocio en particular.

Las mejores prácticas utilizadas en seguridad de la información pueden encontrarse en estándares internacionales como la Norma ISO 27001 que ya fue mencionada anteriormente. Nuestro entrevistado las define como un conjunto de acciones, metodologías, herramientas que se han demostrado que son efectivas en un contexto determinado. Podemos señalar que, teniendo en cuenta lo que nos indicó el especialista, este estándar es el más destacable, ya que tiene una implicancia directa en el management por sentar las bases para la creación de un SGSI, lo que también conlleva desafíos y complejidades en su implementación que pueden ir desde cuestiones administrativas, técnicas, legales, incluso de cultura laboral. Este tema es importante, ya que el personal puede oponer cierta resistencia si sus

actividades se ven modificadas de acuerdo a las que realizaba de manera periódica. Con respecto al proceso de auditoría que se realiza sobre los SGSI, el mismo sigue los lineamientos descriptos en la ISO 27007. Es necesario crear un programa de auditorías para el SGSI, que incluya la frecuencia de las auditorías, métodos, responsabilidades, planeación, así como la forma de entrega de los informes de resultados de dichas auditorías.

Entre otras cosas, en el caso de surgir algún incidente de seguridad, el ingeniero nos señala que se deben llevar a cabo acciones que permitan corregir alguna condición que haya derivado de un incidente, aunque también periódicamente se pueden dar como resultado de otros factores, como auditorías internas, sugerencias, acciones de mejora, revisiones de la alta dirección para dar una solución y erradicar los problemas desde su origen y que los mismos no puedan materializarse nuevamente. Es importante destacar que debe prevalecer un enfoque reactivo en el proceso de gestión de incidentes.

Figura 1 Indicadores – Entrevista a Gerentes Funcionales

	Indicadores	Gerente Funcional de una Big Four (1)	Gerente Funcional de una Big Four (2)	Directora de Operaciones de una Big Four
1	Conocimiento y aplicación de las Normas ISO	Según política de la Casa Matriz	Según política de la Firma	Según política e ISO 27001
2	Controles que aplican a su equipo para observar el cumplimiento de las normas y medidas	Control de accesos, monitoreo de información	Control de emails, monitoreo de información	Control de accesos, antivirus
3	Dificultad en la adaptación de las nuevas practicas	Permisos especiales	Según solicitud del cliente	No se deben modificar
4	Comunicación de las mejores prácticas a los grupos de trabajo	Charlas periódicas	Comunicaciones periódicas vía email	Comunicaciones periódicas vía Intranet
5	Planes de capacitación		Cursos online	Cursos de capacitación y refuerzo
6	Características de la información en el trabajo diario	Información restringida	Información crítica, confidencial y sensible	Confidencialidad, Integridad, Disponibilidad
7	Percepción de los riesgos posibles en la actividad diaria	Identificación simple	Identificación simple	Identificación simple / Confianza en el empleado
8	Plan de acción ante un incidente de seguridad	No tiene conocimiento	No tiene conocimiento	Escalamiento y comunicación, colección de evidencia y posterior remediación
9	Medidas correctivas después de un incidente de seguridad	No tiene conocimiento	Revisión de controles	Revisión de controles

Fuente: Elaboración propia

Figura 2 Indicadores – Entrevista a Especialistas IT

	Indicadores	Especialista IT de una Big Four (1)	Especialista en Seguridad de la Información certificado en ISO 27001
10	Implementación de las Normas ISO en empresas de servicios profesionales	Política	Política
11	Formas de aplicación de los dominios	Controles	Controles
12	Mejores prácticas aplicadas	Medidas que cumplen un estándar (ISO)	Medidas que cumplen un estándar (ISO)
13	Cambios que se deben hacer en el sistema de trabajo según el cliente con el que se trabaje	Cambios según requisitos del cliente (en concordancia con la política)	Cambios según requisitos del cliente (declaración de aplicabilidad)
14	Complejidad de llevar a cabo un SGSI	Equilibrio entre seguridad y rentabilidad del negocio	Cuestiones administrativas, técnicas, legales, de cultura laboral.
15	Planes de capacitación	Comunicación periódica	
16	Medidas técnicas en una implementación de un SGSI	Antivirus, securizacion, manejo de vulnerabilidad	Antivirus, controles
17	Formas de análisis de riesgos	Probabilidad de ocurrencia e impacto	Según ISO 27005
18	Medidas correctivas después de un incidente de seguridad	Aislamiento, investigación, implementación de controles	Investigación, implementación de controles
19	Características del proceso de auditoria	Evidencia de controles	ISO 27007

Fuente: Elaboración propia

3.4 Análisis OSGOOD

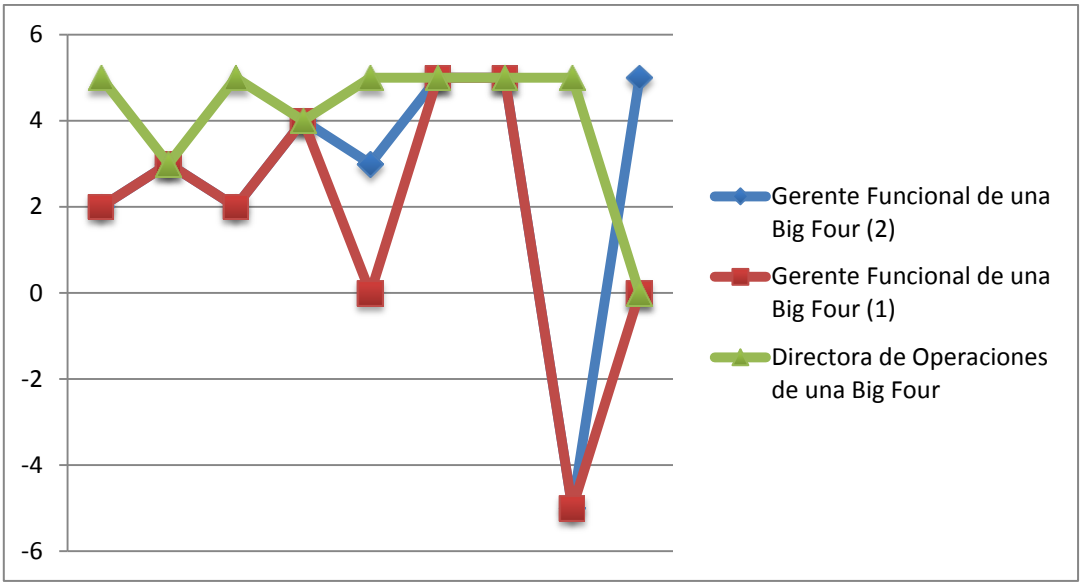
Figura 3 Indicadores Osgood - Entrevista a Gerentes Funcionales

	Indicadores	Gerente Funcional de una Big Four (1)	Gerente Funcional de una Big Four (2)	Directora de Operaciones de una Big Four
1	Conocimiento y aplicación de las Normas ISO	2	2	5
2	Controles que aplican a su equipo para observar el cumplimiento de las normas y medidas	3	3	3
3	Dificultad en la adaptación de las nuevas practicas	2	2	5
4	Comunicación de las mejores prácticas a los grupos de trabajo	4	4	4
5	Planes de capacitación	0	3	5
6	Características de la información en el trabajo diario	5	5	5
7	Percepción de los riesgos posibles en la actividad diaria	5	5	5
8	Plan de acción ante un incidente de seguridad	-5	-5	5
9	Medidas correctivas después de un incidente de seguridad	-5	5	5

*Los que tienen valor “0” indican que los entrevistados no emitieron opinión al respecto.

Fuente: Elaboración propia

Figura 4 Grafico Osgood - Entrevista a Gerentes Funcionales



Fuente: Elaboración Propia

Como puede observarse en el gráfico, en lo que respecta a la variable de Mejores Prácticas en Seguridad de la Información, los indicadores tienden a ser uniformes, con pequeñas variaciones entre ellos. Esto empieza a cambiar cuando nos acercamos a la variable de Grado de implementación y cumplimiento, en el cual se puede ver grandes diferencias entre las respuestas de los gerentes funcionales y directora de operaciones, lo que indica un posible problema de comunicación.

3.4.1 Conocimiento y aplicación de las Normas ISO

Las normas ISO son conocidas por la directora de operaciones, que entiende que la misma se desprende de la política de la casa matriz, por lo tanto cumple con un estándar internacional. En cuanto a los mandos medios, ambos entrevistados coinciden en que se aplican políticas que provienen de la casa matriz a nivel internacional, pero no mencionan acerca del conocimiento de las Normas ISO.

3.4.2 Controles que aplican a su equipo para observar el cumplimiento de las normas y medidas

Los controles que se llevan a cabo son en su mayoría tendientes a proteger la confidencialidad de la información con la que se trabaja. Entre los principales

controles que se mencionan encontramos: control de accesos, control y monitoreo de la información que se envía por email, sistemas de antivirus, entre otros.

3.4.3 Dificultad en la adaptación de las nuevas practicas

Si bien la directora de operaciones indica que el nivel de seguridad nunca puede ni debe ser alterado y que no deberían aplicarse nuevas medidas al trabajar con nuevos clientes por lo general, los gerentes funcionales coinciden en que podrían llegar a ser solicitados por estos clientes, y que deben obtenerse permisos especiales para acceder a determinada información de los mismos, lo que indica que siempre el entorno de seguridad se mantiene y que ningún cambio afecta la política con la que trabaja la empresa.

3.4.4 Comunicación de las mejores prácticas a los grupos de trabajo

Todas las medidas adoptadas se comunican a los empleados mediante comunicaciones, ya sea en charlas, vía email o vía intranet de la empresa. Es importante destacar que los tres entrevistados coincidieron en la periodicidad de las mismas.

3.4.5 Planes de capacitación

Se realizan cursos de capacitación para los nuevos empleados antes de comenzar a trabajar con información de clientes, y a su vez se realizan diversos cursos online en formato e-learning para reforzar los conceptos en forma periódica.

3.4.6 Características de la información en el trabajo diario

La información con la que se trabaja, ya sea propia o de clientes se caracteriza por ser información restringida, critica, confidencial y sensible, que incide en gran medida en la toma de decisiones. A su vez se destaca que las características que quiere preservarse de la misma son confidencialidad, integridad y disponibilidad.

3.4.7 Percepción de los riesgos posibles en la actividad diaria

Los tres entrevistados coinciden en que la identificación de los riesgos en la actividad diaria es simple, dado que los riesgos en general siempre son los mismos, aunque en algunos casos cuesta un poco más el control. También se menciona un

principio de confianza en el empleado, ya que el principal riesgo proviene de factores internos de la empresa.

3.4.8 Plan de acción ante un incidente de seguridad

En este punto notamos una discordancia entre los dos tipos de perfiles analizados, ya que ambos gerentes funcionales entrevistados afirman no tener conocimiento acerca de los planes de acción formales ante un incidente de seguridad, debido a que nunca han tenido que enfrentar uno. Señalan que se valdrían puramente de su experiencia, conocimiento y criterio profesional. En contrapartida, la directora de operaciones explica que si existen planes formales con tareas, procedimientos y roles bien definidos, lo que evidencia un problema de comunicación entre la alta dirección y los mandos medios.

3.4.9 Medidas correctivas después de un incidente de seguridad

Las medidas correctivas después de un incidente de seguridad se basan en una revisión de los controles que se llevaron a cabo, y siempre se busca identificar las causas para que el mismo no vuelva a ocurrir.

3.5 Análisis de las encuestas

3.5.1 Segmentación de la muestra

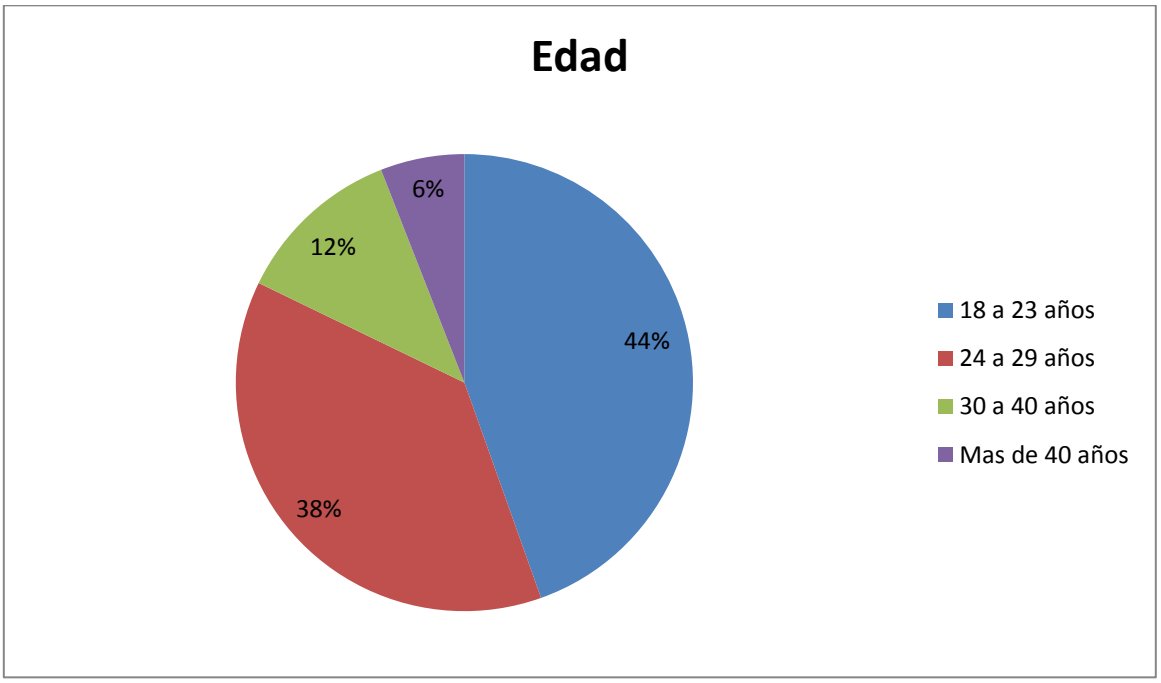
3.5.1.1 Edad

Para nuestro estudio de campo hemos realizado 125 encuestas a diversos empleados de las cuatro empresas de servicios profesionales más importantes a nivel mundial.

La muestra está compuesta de la siguiente forma 56 empleados que tienen entre 18 y 23 años que conforman el 45% de la muestra. El número de encuestados de esta edad es mayor a la de los otros segmentos porque en estas empresas se caracterizan por tener gran cantidad de empleados jóvenes. El segundo segmento más elevado es el de los empleados que tienen entre 24 y 25 años que representan el 38%. Los

segmentos de edades de entre 30 y 40 años y más de 40 forman el 12% y 7% respectivamente.

Edad	18-23	%	24-29	%	30-40	%	Más 40	%
Cantidad de personas	56	45%	47	38%	15	12%	7	6%
Total	56	45%	47	38%	15	12%	7	6%



3.5.1.2 Puesto que ocupan

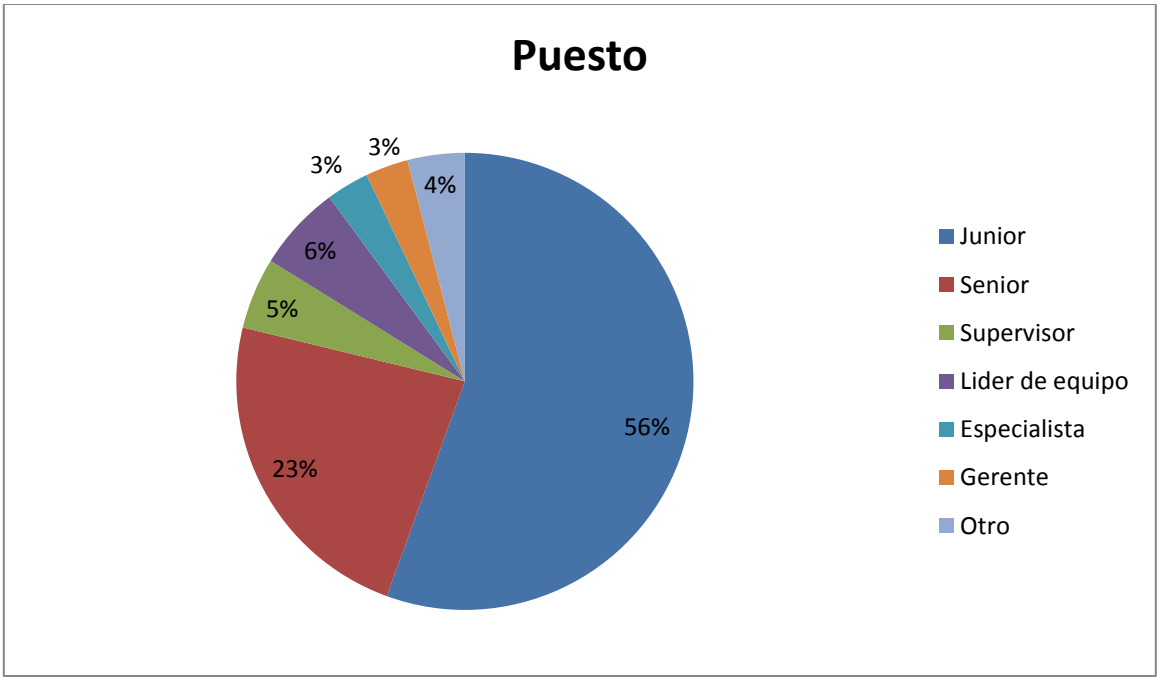
La segunda forma en la que se clasificaron los datos es según el puesto que ocupan los mismos. El 55% lo representan los junior que son las personas que recién inician en la empresa y que todavía están terminando su carrera universitaria o se han recibido hace menos de dos años.

El 23% de la muestra lo componen los sénior, este puesto lo ocupan las personas con experiencia de entre 3 a 5 años en el área que están trabajando son personas que pudieron haber iniciado su carrera profesional en la empresa o que han entrado

ya con esa categoría. El otro grupo con mayor porcentaje es el compuesto por los líderes de equipo, este grupo representa el 6% de la muestra. Las personas que ocupan este puesto se encargan de la coordinación de grupos de juniors y semi-seniors, ellos asignan las tareas y controlan la actividad de forma más operativa.

El resto de la muestra está compuesto por supervisores, especialistas y gerentes que representan el 5%, 3% y 3% respectivamente. El 4% restante lo componen otros puestos como jóvenes profesionales, pasantes y técnicos.

Puesto	Junior		Senior		Supervisor		Líder de eq.		Especialista		Gerente		Otros	
Cantidad de personas	69	55%	29	23%	6	5%	8	6%	4	3%	4	3%	5	4%
Total	69	55%	29	23%	6	5%	8	6%	4	3%	4	3%	5	4%



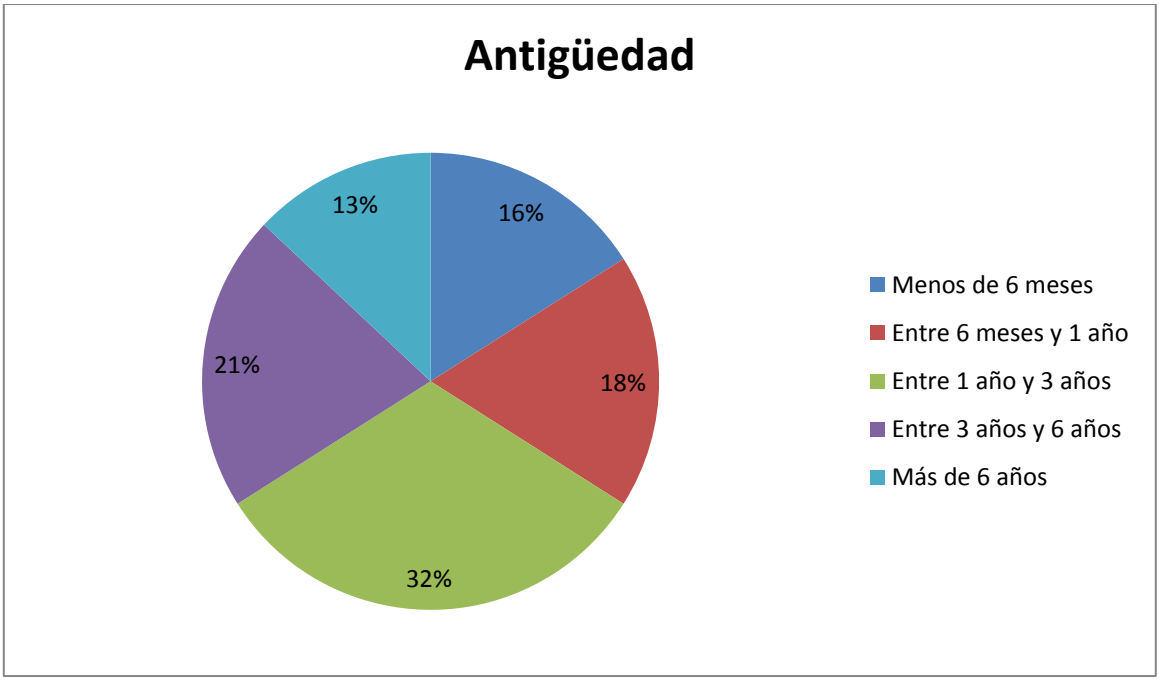
3.5.1.3 Antigüedad

Otro aspecto clave a analizar en la muestra es la antigüedad que tienen los empleados en las empresas en las que se realizó la encuesta. Este aspecto es relevante ya que al ser la seguridad de la información un tipo de política y aspecto en el que se busca profesionalizar al empleado, se puede evaluar de esta forma como está incorporada el conocimiento de estas normas según la antigüedad que tiene el empleado.

La muestra está compuesto principalmente por empleados que tienen entre 1 año y 3 años en la empresa. Este grupo representa el 32% de la muestra. El segundo grupo más relevante es el que lleva entre 3 y 6 años trabajando en este tipo de empresas.

El tercer grupo más importante es de las personas que tienen una antigüedad de entre 6 meses y un año que conforman el 18%. El porcentaje restante lo componen las personas con más de 6 años en la empresa y con menos de 6 meses que conforman 13% y 16%.

Antigüedad	Menos 6 meses		6 Meses a 1 Año		1 a 3 Años		3 a 6 Años		Más de 6 Años	
Cantidad de personas	20	16%	23	18%	40	32%	26	21%	16	13%
Total	20	16%	23	18%	40	32%	26	21%	16	13%



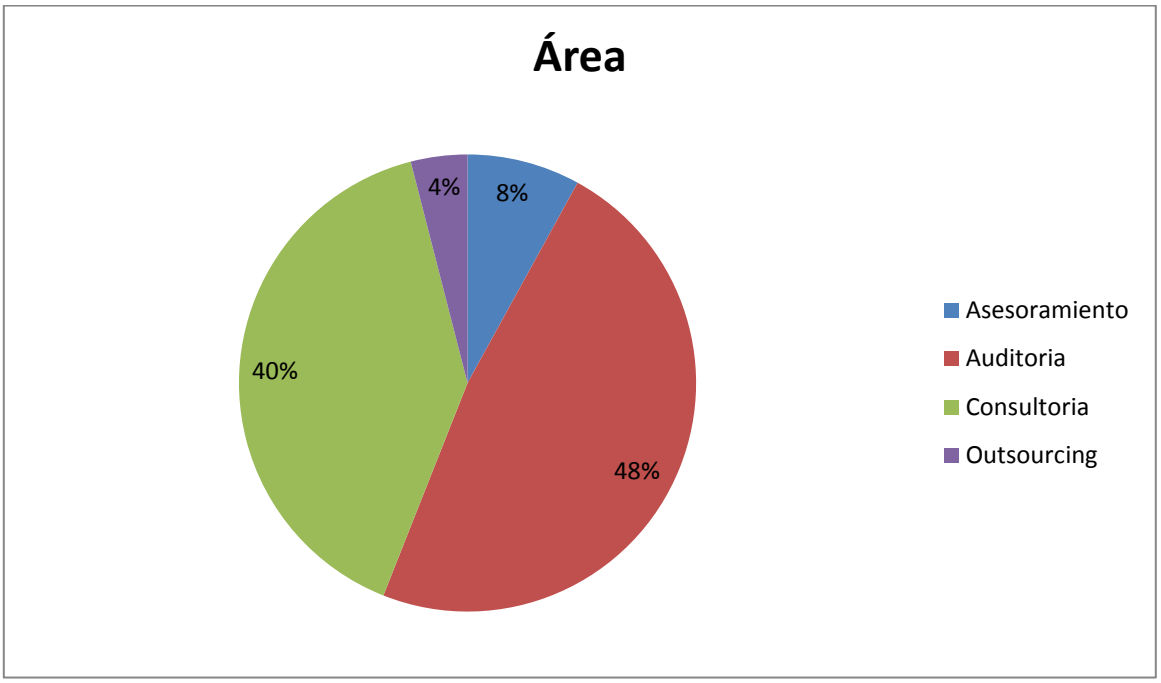
3.5.1.4 Área en la que trabaja

Otro aspecto clave a analizar es el área en el que trabajan los encuestados. Consideramos que este aspecto es relevante ya que según el área en el que trabajan es el tipo de información al cual pueden acceder y el tipo de tratamiento que le deben dar.

Las áreas en las que más enfocamos las encuestas son auditoría y consultoría, dado que son las áreas en las que las empresas más se destacan en el mercado y en donde deben brindar la mayor excelencia. Estas áreas componen el 48% y 40% de la muestra.

Las otras áreas en las que también se maneja información clave y tuvimos en cuenta en nuestro estudio son asesoramiento legal e impositivo que compone el 8% de la muestra seguido por Outsourcing que compone el 4% de la muestra.

Área	Asesoramiento		Auditoria		Consultoría		Outsourcing	
Cantidad de personas	10	8%	60	48%	50	40%	5	4%
Total	10	8%	60	48%	50	40%	5	4%

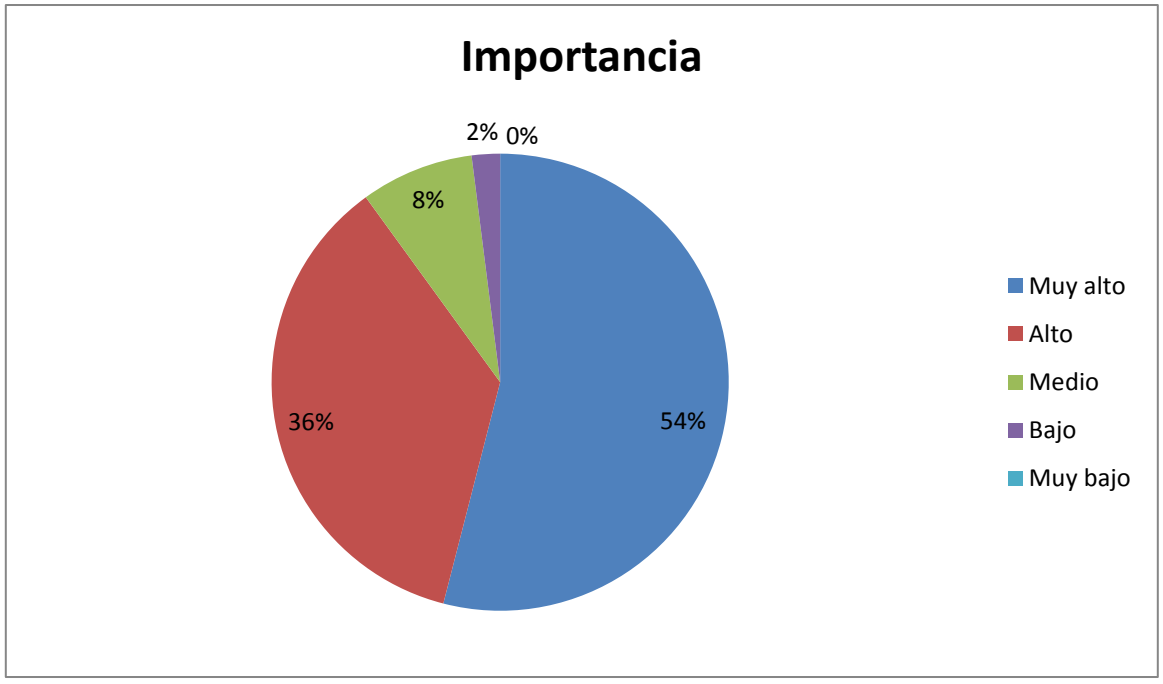


3.5.2 Aspectos analizados

3.5.2.1 Grado de importancia que se le da a la información del cliente en su actividad diaria laboral

El objetivo que planteábamos analizar con esta pregunta es la importancia que le dan los empleados a la información que obtienen de los clientes para su actividad diaria. Las respuestas obtenidas fueron las siguientes:

Grado de importancia	Empleados	%
Muy alto	68	54%
Alto	45	36%
Medio	10	8%
Bajos	2	2%
Muy bajo	0	0%



Lo que podemos analizar en este ítem es que el 54% de los empleados consideran que la información obtenida de los clientes es sumamente clave para su trabajo y el 36% consideran que el grado de importancia que le dan a la información es alto. Esto

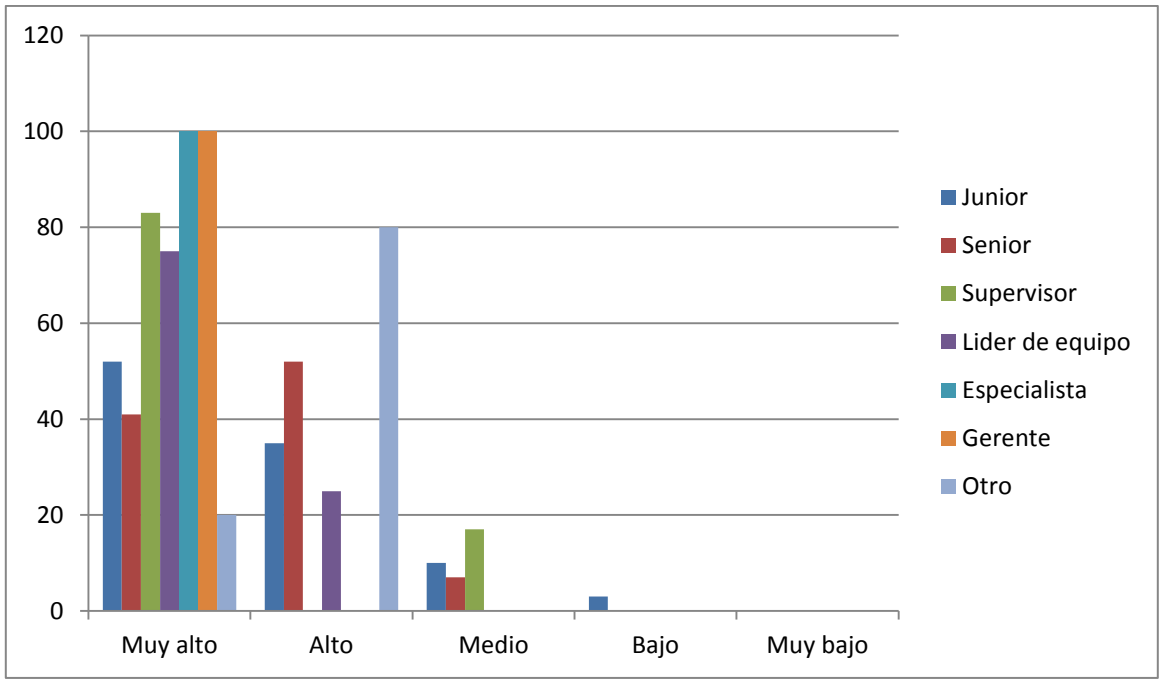
se debe a que los encuestados trabajan en empresas que los asignan por proyectos y sus actividades se basan en realizar actividades en empresas a los que los asignan.

El porcentaje restante está compuesto por personas que consideran la información con grado de importancia media que es del (8%) y el 2% restante es de las personas que consideran el grado de importancia baja. Ninguno de los encuestados considero que el grado de importancia es muy bajo.

Estos resultados son claves para continuar nuestro análisis ya que podemos proseguir el análisis de las medidas de protección que le dan las empresas a la información que manejan. Evaluando el trato especial que se le debe dar a la misma. (Marco teórico importancia de la información).

Si analizamos los resultados basándonos en el puesto que ocupan los empleados los resultados se pueden analizar de la siguiente forma.

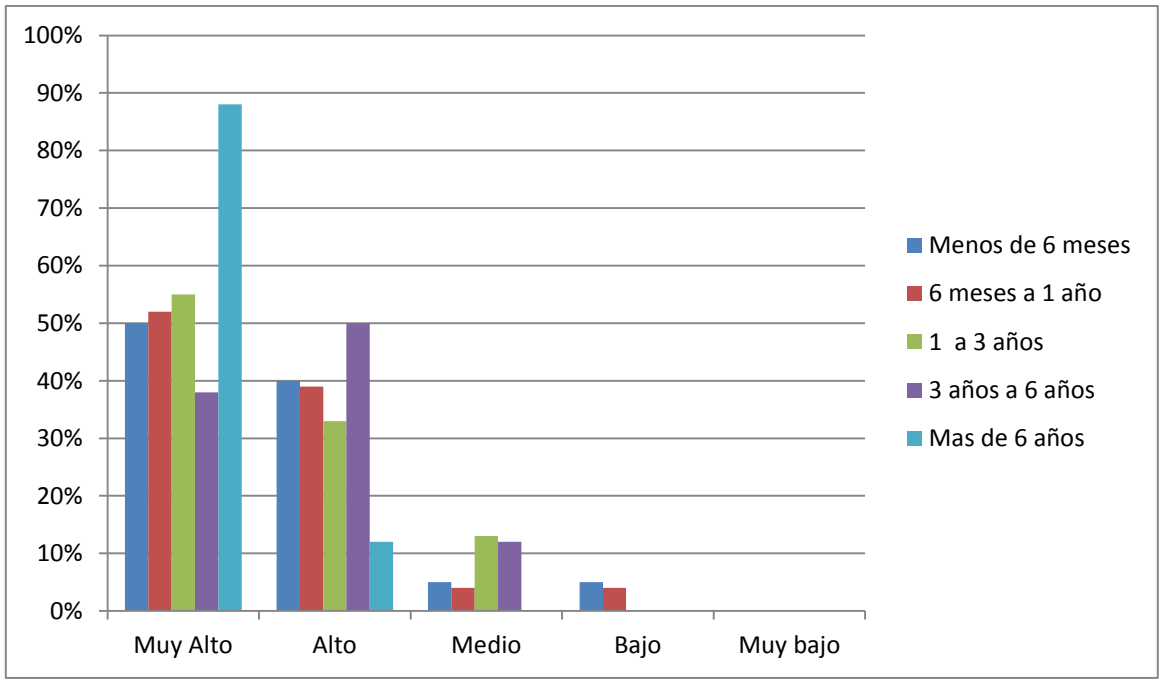
Importancia a la información	Junior		Senior		Supervisor		Lider de equipo		Especialista		Gerente		Otros	
Muy alto	36	52%	12	41%	5	83%	6	75%	4	100%	4	100%	1	20%
Alto	24	35%	15	52%	0	0%	2	25%	0	0%	0	0%	4	80%
Medio	7	10%	2	7%	1	17%	0	0%	0	0%	0	0%	0	0%
Bajo	2	3%	0	0%	0	0%	0	0%	0	0%	0	0%	0	0%
Muy bajo	0	0%	0	0%	0	0%	0	0%	0	0%	0	0%	0	0%



Lo relevante que podemos destacar con este análisis es que los cargos más altos (Especialistas y Gerentes) consideran que el 100% de la información que manejan en sus actividades tienen un grado de importancia muy alto. A medida que se va disminuyendo el nivel jerárquico se va diversificando y esto se debe a que no están tan en contacto con el cliente y la información a la que acceden se ve limitada por los rangos superiores.

Otro aspecto que también se debe considerar es que al ser cargos que tienen menos experiencia en la vida laboral también desconocen el riesgo que hay detrás de esta información por ende deben tener un acceso más limitado.

Importancia a la información	Menos 6 meses		6 Meses- 1 Año		1 Año- 3 Año		3 años - 6 años		Mas 6 años	
Muy alto	10	50%	12	53%	22	55%	10	38%	14	88%
Alto	8	40%	9	39%	13	32%	13	50%	2	12%
Medio	1	5%	1	4%	5	13%	3	12%	0	0%
Bajo	1	5%	1	4%	0	0%	0	0%	0	0%
Muy bajo	0	0%	0	0%	0	0%	0	0%	0	0%

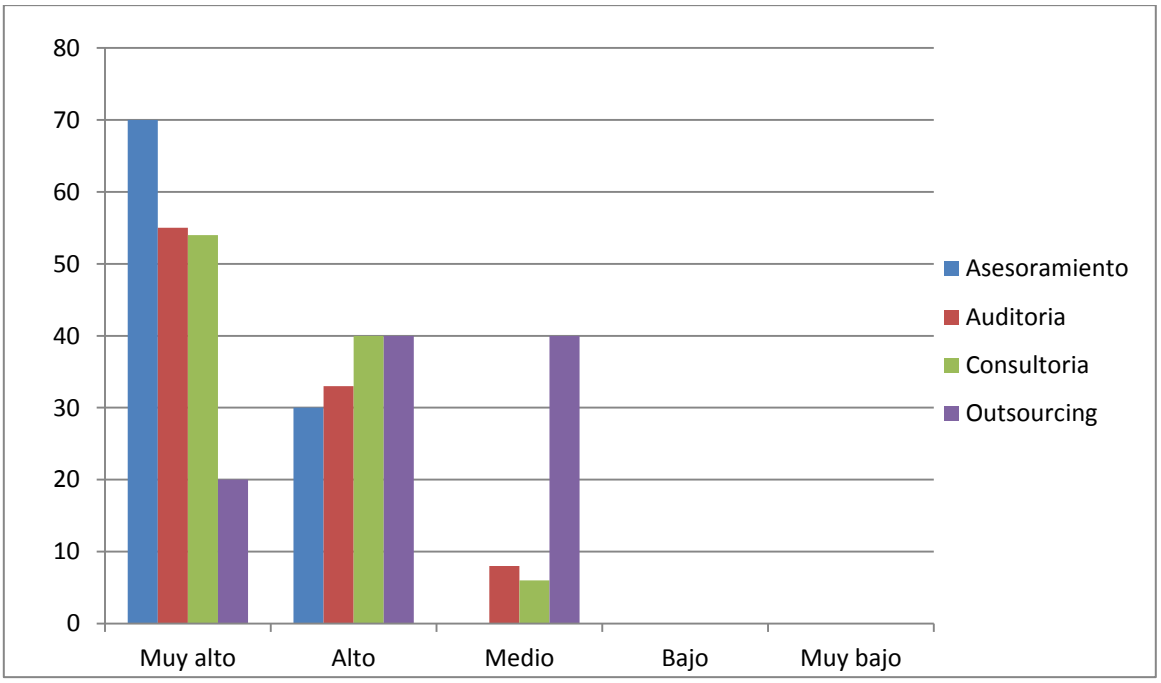


Si analizamos los grados de información más importantes (muy alto y alto) se caracteriza por estar compuesto por 90% menos de 6 meses, 92% entre 6 meses y un año, 87% entre un año y tres años, 88% entre 3 años y 3 años y 100% cuando tienen más de 6 años.

Haciendo este análisis podemos llegar a la conclusión de que las personas que tienen mayor antigüedad son las que grado de importancia le dan a la información. Las personas que le indicaron a la información los grados más chicos son aquellas que tienen menor antigüedad lo cual coincidiría en el hecho de que aún no conocen la forma de trabajo y las políticas que tienen la empresa.

El grado de importancia medio es solo utilizado en las personas cuya antigüedad es menor de 6 años. Lo cual implica que mientas más ascienden en el cargo jerárquico mayor relevancia se le da a la información.

Importancia a la información	Asesoramiento		Auditoria		Consultoría		Outsourcing	
Muy alto	7	70%	33	55%	27	54%	1	20%
Alto	3	30%	20	33%	20	40%	2	40%
Medio	0	0%	5	8%	3	6%	2	40%
Bajo	0	0%	2	3%	0	0%	0	0%
Muy bajo	0	0%	0	0%	0	0%	0	0%



Si analizamos las respuestas segmentando por área en la que trabajan podemos decir que en el área de asesoramiento el 70% considera que la información con un grado muy alto y el restante alto. Para el área de auditoria los porcentajes son más dispersos ya que el 55% considera que es muy alto, el 33% alto, el 8% medio y el 3% bajo. Este aspecto de análisis es relevante ya que la información que maneja el sector de auditoria es relevante para la empresa a nivel financiero y para los mercados (ver marco teórico las big four y la información que manejan)

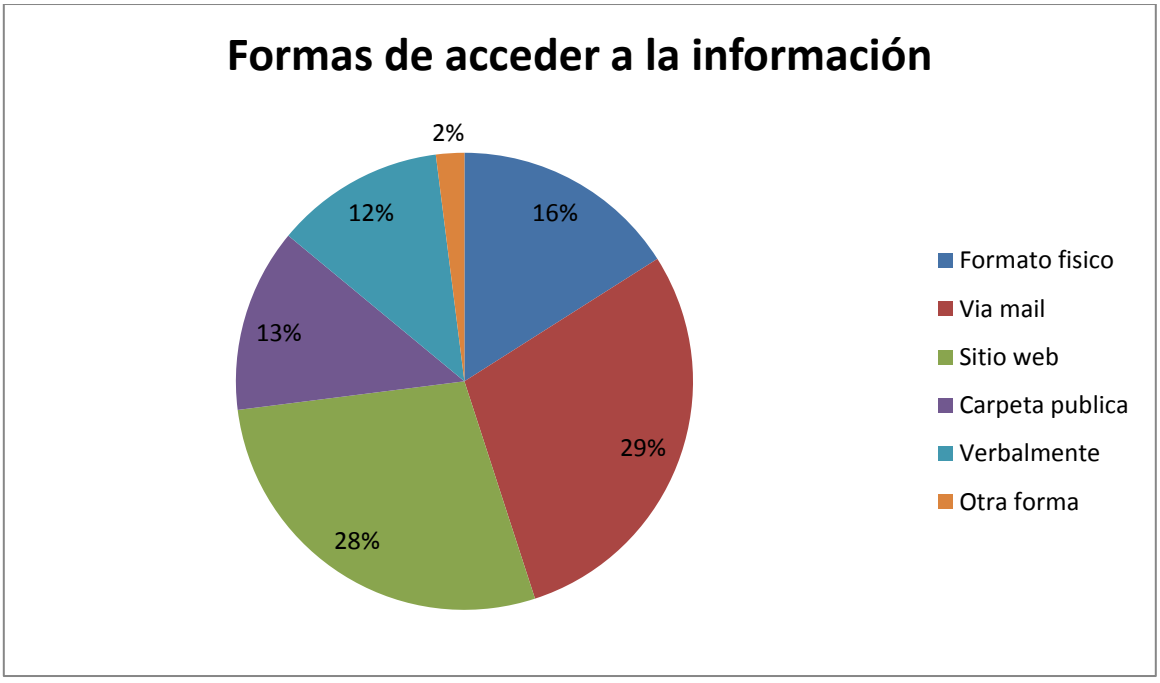
En el sector de consultoría, la información se dispersa en los grados más elevados y un porcentaje del 6% para el grado de importancia medio. Lo cual le otorga el 54% al grado de importancia muy alto y 40% al alto.

En Outsourcing el porcentaje se segmenta entre los primeros tres niveles, aunque el porcentaje es más parejo en las opciones alto y medio. El grado de importancia muy alto solo es considerado por el 20% de los encuestados.

3.5.2.2 Formas en las que accede a la información de los clientes con los que trabaja

Dado que uno de los aspectos que ha complejizado la seguridad de la información es las formas en las cuales las personas pueden acceder a la información consideramos relevante evaluar cuáles son las vías de acceso más comunes.

Formas de acceso a la información	Personas	%
Me dan la información en formato físico	50	16%
Me envían la información por mail	93	29%
Sitio web en el que se encuentra disponible	87	28%
Se encuentra en una carpeta publica	42	13%
Me lo informan verbalmente	38	12%
Otro	6	2%



Del análisis obtenido podemos saber que el 16% de los encuestados tienen la información en formato físico, el 29% vía mail, el 28% tiene la información en un sitio web al cual accede para descargar la información mientras que el 13% lo tienen en una carpeta publica a la cual accede.

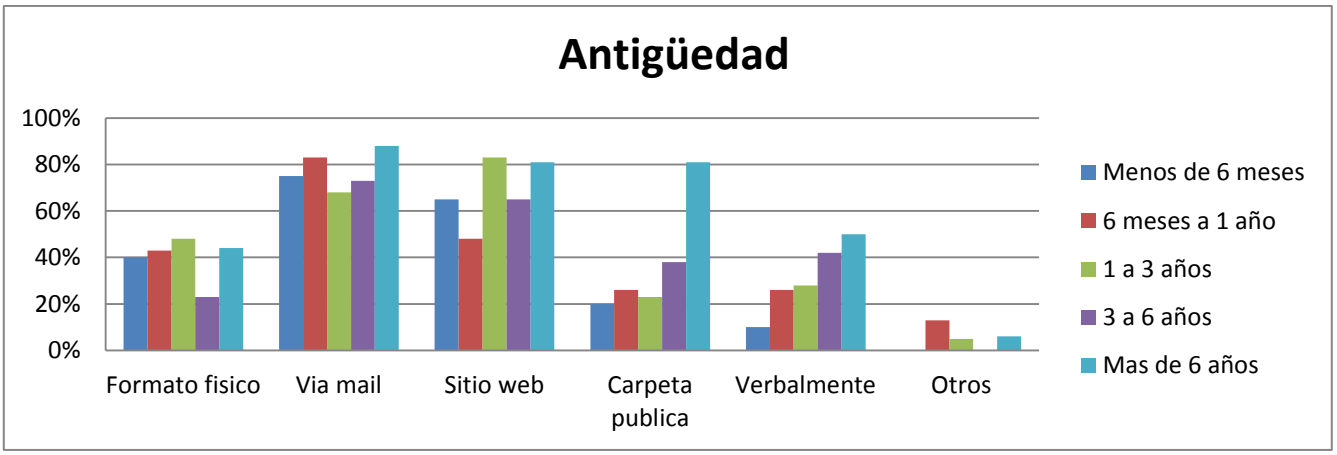
La información es brindada verbalmente para el 12% de los encuestados y un 2% utiliza otras formas las cuales entre ellas se encuentra sistemas de información, reuniones con los clientes, discos virtuales compartidos por el proyecto y la computadora del cliente.

Si analizamos este aspecto según el puesto que ocupa, la antigüedad y la categoría podemos ver los siguientes datos:

Antigüedad / Formas de acceso	Menos 6 meses		6 meses a 1 año		1 año a 3 años		3 años a 6 años		Mas 6 años	
Me dan la información en formato físico	8	40%	10	43%	19	48%	6	23%	7	44%
Me envían la información por mail	14	75%	19	83%	27	68%	19	73%	14	88%
Sitio web en el que se encuentra disponible	13	65%	11	48%	33	83%	17	65%	13	81%
Se encuentra en una carpeta publica	4	20%	6	26%	9	23%	10	38%	13	81%
Me lo informan verbalmente	2	10%	6	26%	11	28%	11	42%	8	50%
Otro	0	0%	3	13%	2	5%	0	0%	1	6%

Si nos guiamos por la antigüedad que tienen los empleados podemos evaluar que no es uniforme para la antigüedad que tiene cada empleado podemos ver que esta no es uniforme a que en el caso de formato físico. La forma que más se utilizan en los empleados con una antigüedad menor de 6 meses son él envió vía mail y un sitio web común. Esta forma también coincide con las respuestas dadas por los otros segmentos excepto en el caso de uno a tres años.

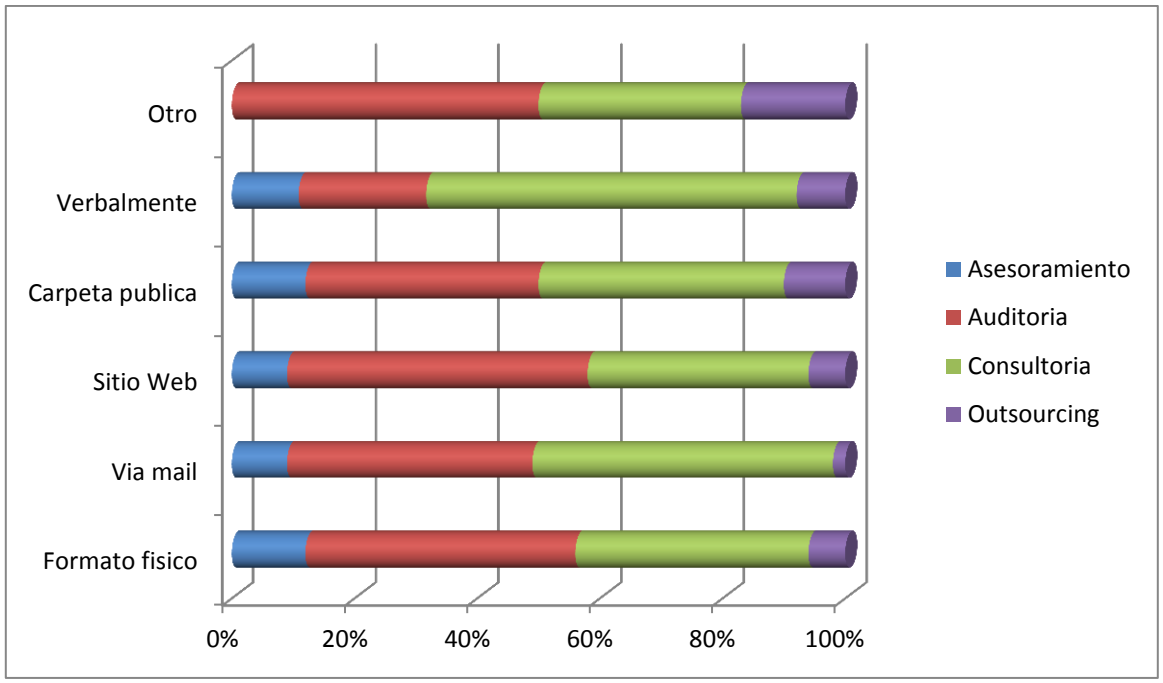
Entre las formas menos comunes coinciden la de informa verbalmente en todos los segmentos excepto en los que tienen más de 6 años que tienen la información en formato físico.



Si nos guiamos por la antigüedad que tienen los empleados podemos evaluar que no es uniforme para la antigüedad que tiene cada empleado podemos ver que esta no es uniforme a que en el caso de formato físico. La forma que más se utilizan en los empleados con una antigüedad menor de 6 meses son él envió vía mail y un sitio web común. Esta forma también coincide con las respuestas dadas por los otros segmentos excepto en el caso de uno a tres años.

Entre las formas menos comunes coinciden la de informa verbalmente en todos los segmentos excepto en los que tienen más de 6 años que tienen la información en formato físico.

Área / Formas de acceso	Asesoramiento		Auditoria		Consultoría		Outsourcing	
Me dan la información en formato físico	6	12%	22	44%	19	38%	3	6%
Me envían la información por mail	8	9%	37	40%	46	49%	2	2%
Sitio web en el que se encuentra disponible	8	9%	43	49%	31	36%	5	6%
Se encuentra en una carpeta publica	5	12%	16	38%	17	40%	4	10%
Me lo informan verbalmente	4	11%	8	21%	23	61%	3	8%
Otro	0	0%	3	50%	2	33%	1	17%

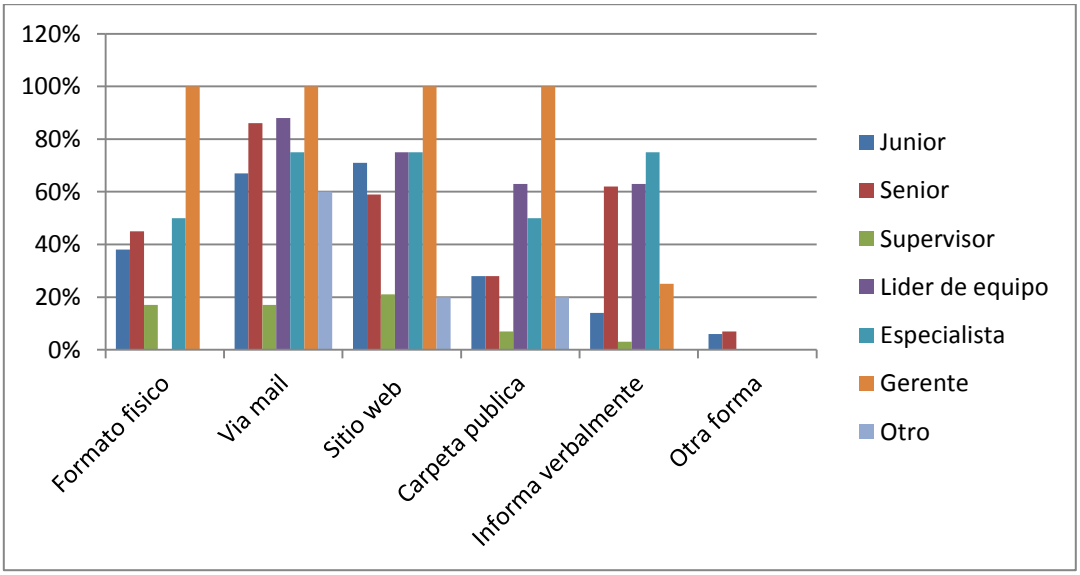


El aspecto de la forma en que se da la información difiere mucho según el área en el que trabaja el empleado. Por eso en el caso de formato físico quien predomina es el área de auditoria al igual que en que la información se encuentre en sitios web (Ej. Comisión nacional de valores) y acceder a información que se encuentran cargadas en computadoras de los clientes.

Asesoramiento tiene una distribución más pareja y las formas más utilizadas son información en formato físico y carpeta pública. Para el área de Consultoría las formas más comunes es la comunicación verbal y la información vía mail. En el área de Outsourcing las formas más comunes son totalmente distintas a las que se utilizan en las empresas en estos se utilizan las reuniones como forma de conocer mejor al cliente.

Si analizamos la forma de acceder a la información basándonos en el puesto que ocupa podemos obtener la siguiente información:

Puesto / Formas de acceso	Junior		Senior		Supervisor		Lieder de equipos		Especialista		Gerente		Otros	
Me dan la información en formato físico	26	38%	13	45%	5	17%	0	0%	2	50%	4	100%	0	0%
Me envían la información por mail	46	67%	25	86%	5	17%	7	88%	3	75%	4	100%	3	60%
Sitio web en el que se encuentra disponible	49	71%	17	59%	6	21%	6	75%	3	75%	4	100%	1	20%
Se encuentra en una carpeta publica	19	28%	8	28%	2	7%	5	63%	2	50%	4	100%	1	20%
Me lo informan verbalmente	10	14%	18	62%	1	3%	5	63%	3	75%	1	25%	0	0%
Otro	4	6%	2	7%	0	0%	0	0%	0	0%	0	0%	0	0%



En el caso de los juniors la vía que más se utiliza son los sitios webs lo que tiene mayor sentido ya que al ser mayor la cantidad de empleados en esta categoría es necesario obtener un mayor control y de esta forma se puede controlar y ver qué información descargo. En el caso de los seniors la forma de acceder a la información más común es vía mail al igual que ara los líderes de equipos y especialistas.

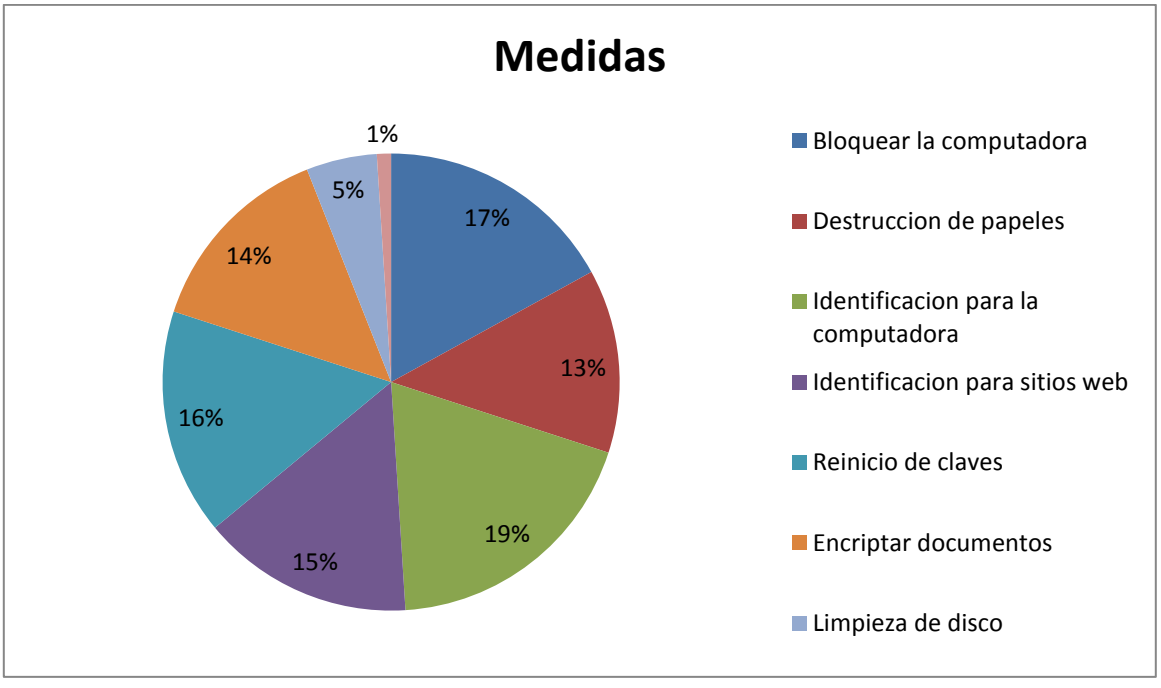
Los especialistas tienen una distribución más pareja que permite ver que utilizan distintos tipos en los que se encuentra la información. En el caso de los gerentes

sucede un caso bastante particular ya que la mayoría contesto que utilizan todos los posibles formatos sin embargo el que menos utilizan es la comunicación verbal.

3.5.2.3 Medidas que considera que aplica el personal de la empresa donde usted trabaja o trabajó para proteger la información

Lo que buscamos con esta pregunta es evaluar el conocimiento que tienen los empleados de las normas de seguridad que utilizan en las empresas.

Medidas	Personas	%
Bloquear la computadora	106	17%
Destrucción de papeles confidenciales	82	13%
Solicitud de contraseñas para la computadora	120	19%
Solicitud de contraseñas para sitios web	93	15%
Reiniciar la contraseña cada tres meses	101	16%
Encriptación de documentos/pendrives	90	14%
Limpieza de documentos en disco	38	5%
Otros	6	1%

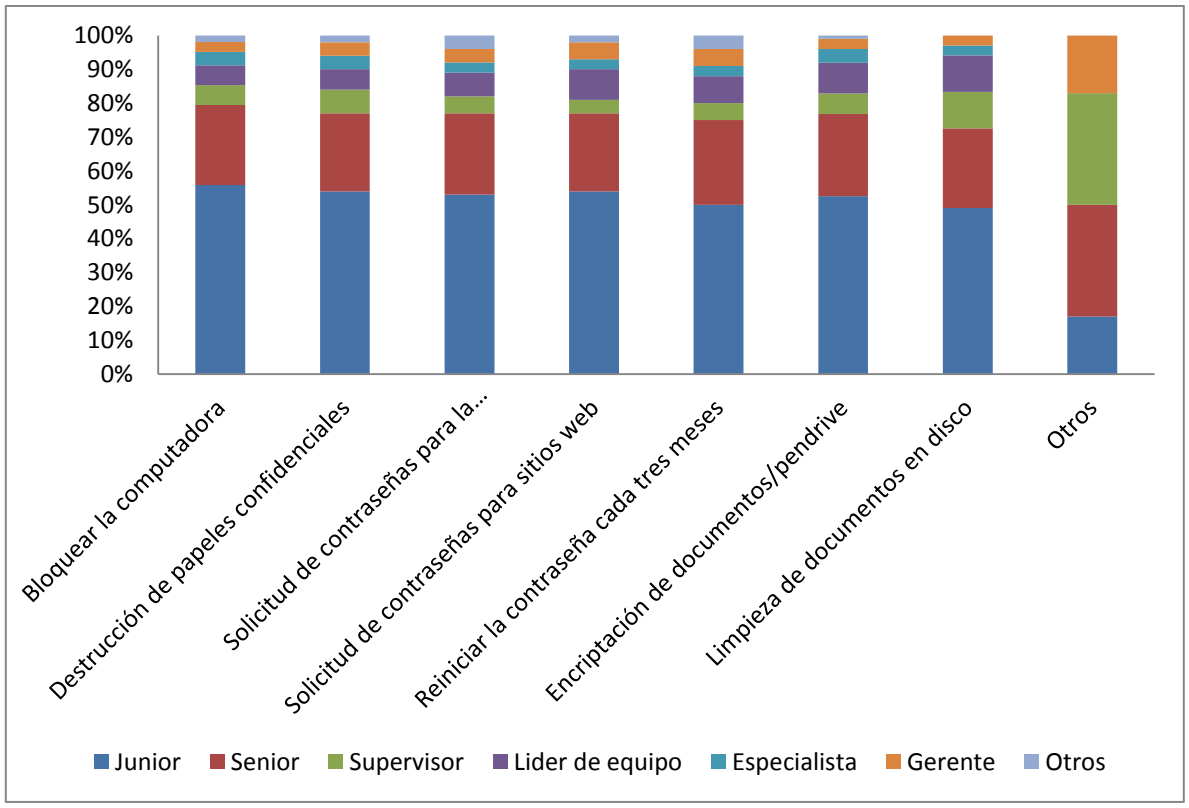


Lo que podemos ver en este aspecto que los empleados más destacan como norma de seguridad es la identificación al momento de ingresar a las computadoras (19%) que viene relacionado con la otra medida de seguridad que es bloquear la computadora cada vez que se alejan del sitio de trabajo que compone el 17%

Las otras medidas más importantes fueron reiniciar la computadora cada tres meses que compone el 16%, solicitud de contraseñas para sitios web el 15%, encriptación de documentos/pendrive que representa el 14% y destrucción de papeles confidenciales el 13%.

Las medidas que menos influyen son la limpieza automática del disco y bloque del proxy y no acceder a la red de la empresa con cualquier dispositivo.

Puesto / Medidas	Junior		Senior		Supervisor		Líder de equipo		Especialista		Gerente		Otros	
Bloquear la computadora	60	57%	25	24%	6	6%	6	6%	4	4%	3	3%	2	2%
Destrucción de papeles confidenciales	44	54%	19	23%	6	7%	5	6%	3	4%	3	4%	2	2%
Solicitud de contraseñas para la computadora	63	53%	29	24%	6	5%	8	7%	4	3%	5	4%	5	4%
Solicitud de contraseñas para sitios web	50	54%	21	23%	4	4%	8	9%	3	3%	5	5%	2	2%
Reiniciar la contraseña cada tres meses	51	50%	25	25%	5	5%	8	8%	3	3%	5	5%	4	4%
Encriptación de documentos/pendrive	47	52%	22	24%	5	6%	8	9%	4	4%	3	3%	1	1%
Limpieza de documentos en disco	19	50%	9	24%	4	11%	4	11%	1	3%	1	3%	0	0%
Otros	1	17%	2	33%	2	33%	0	0%	0	0%	1	17%	0	0%



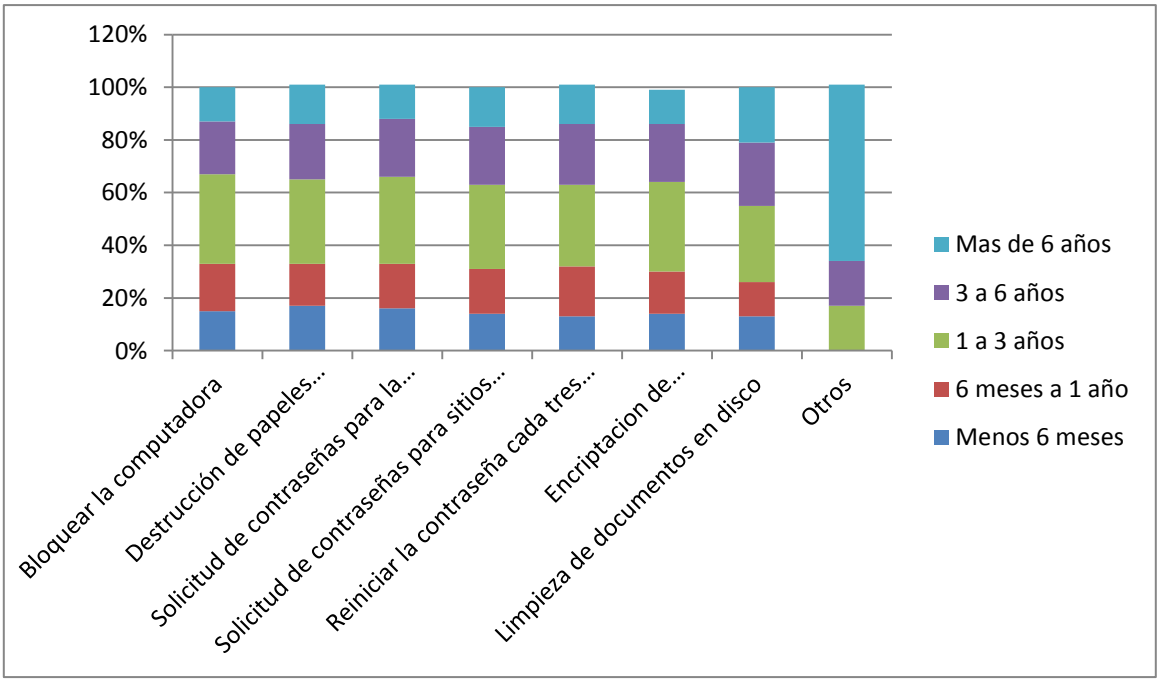
Si evaluamos las medidas que más utilizan los empleados según el puesto que ocupan podemos decir que los juniors la medida que más seleccionaron es bloquear la computadora mientras que los seniors seleccionaron no acceder a sitios con información de la empresa desde cualquier dispositivo móvil.

Los supervisores seleccionaron como la medida más importante la limpieza de disco cada determinado periodo esta medida es relevante ya que en los casos de que el empleado se olvide de eliminar esos archivos con información confidencial la empresa se podrá asegurar de que el empleados no la siga manejando.

En el caso de los líderes de equipo la medida que más seleccionaron fue el borrado de documentos del disco, esta medida difiere de la mencionada por los supervisores porque esta última la debe realizar el empleado y no la realiza la empresa a nivel sistema.

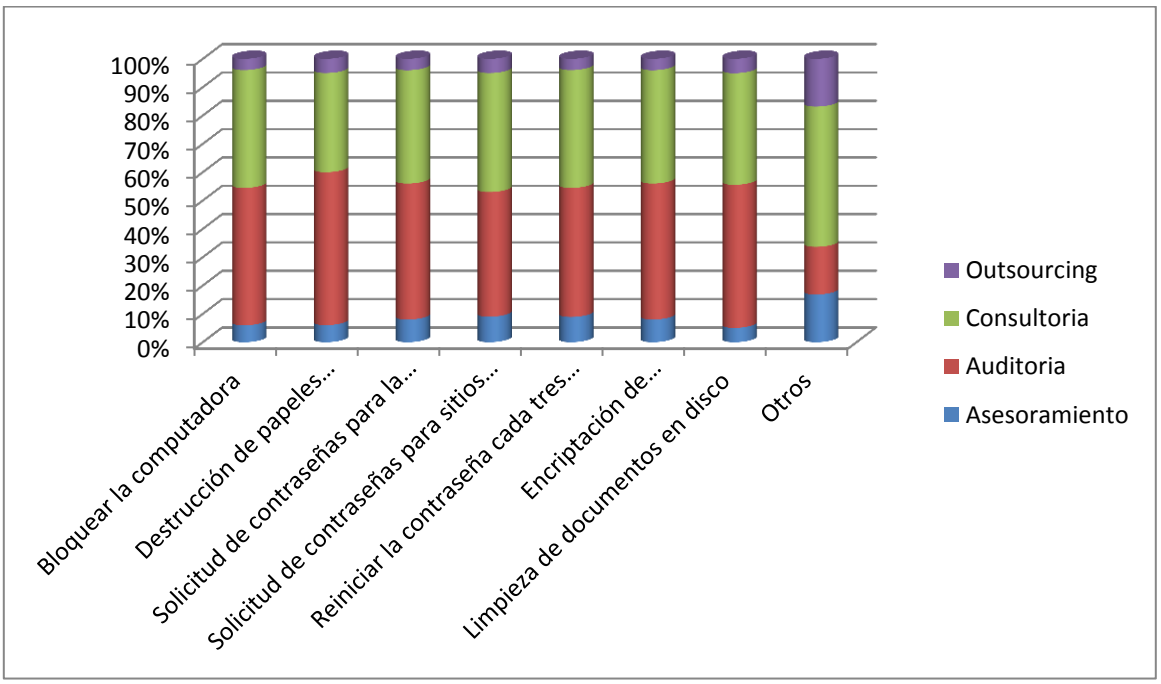
Los especialistas y gerentes marcaron con la misma dispersión las mismas formas de proteger la información en las empresas de servicios profesionales.

Antigüedad / Medidas	Menos 6 meses		6 meses a 1 año		1 a 3 años		3 a 6 años		Mas 6 años	
Bloquear la computadora	16	15%	19	18%	36	34%	21	20%	14	13%
Destrucción de papeles confidenciales	14	17%	13	16%	26	32%	17	21%	12	15%
Solicitud de contraseñas para la computadora	19	16%	20	17%	39	33%	26	22%	16	13%
Solicitud de contraseñas para sitios web	13	14%	16	17%	30	32%	20	22%	14	15%
Reiniciar la contraseña cada tres meses	13	13%	19	19%	31	31%	23	23%	15	15%
Encriptación de documentos/pendrive	13	14%	14	16%	31	34%	20	22%	12	13%
Limpieza de documentos en disco	5	13%	5	13%	11	29%	9	24%	8	21%
Otros	0	0%	0	0%	1	17%	1	17%	4	67%



Analizando las medidas según la antigüedad del personal podemos deducir que en todos los segmentos es similar el porcentaje de aplicación. Lo que se puede evaluar es que en el caso de los empleados con una antigüedad mayor a 6 años son los que tienen medidas de protección distintas al resto del grupo.

Área / Antigüedad	Asesoramiento		Auditoria		Consultoría		Outsourcing	
Bloquear la computadora	6	6%	52	49%	44	42%	4	4%
Destrucción de papeles confidenciales	5	6%	44	54%	29	35%	4	5%
Solicitud de contraseñas para la computadora	9	8%	58	48%	48	40%	5	4%
Solicitud de contraseñas para sitios web	8	9%	41	44%	39	42%	5	5%
Reiniciar la contraseña cada tres meses	9	9%	46	46%	42	42%	4	4%
Encriptación de documentos/pendrives	7	8%	43	48%	36	40%	4	4%
Limpieza de documentos en disco	2	5%	19	50%	15	39%	2	5%
Otros	1	17%	1	16%	3	50%	1	17%



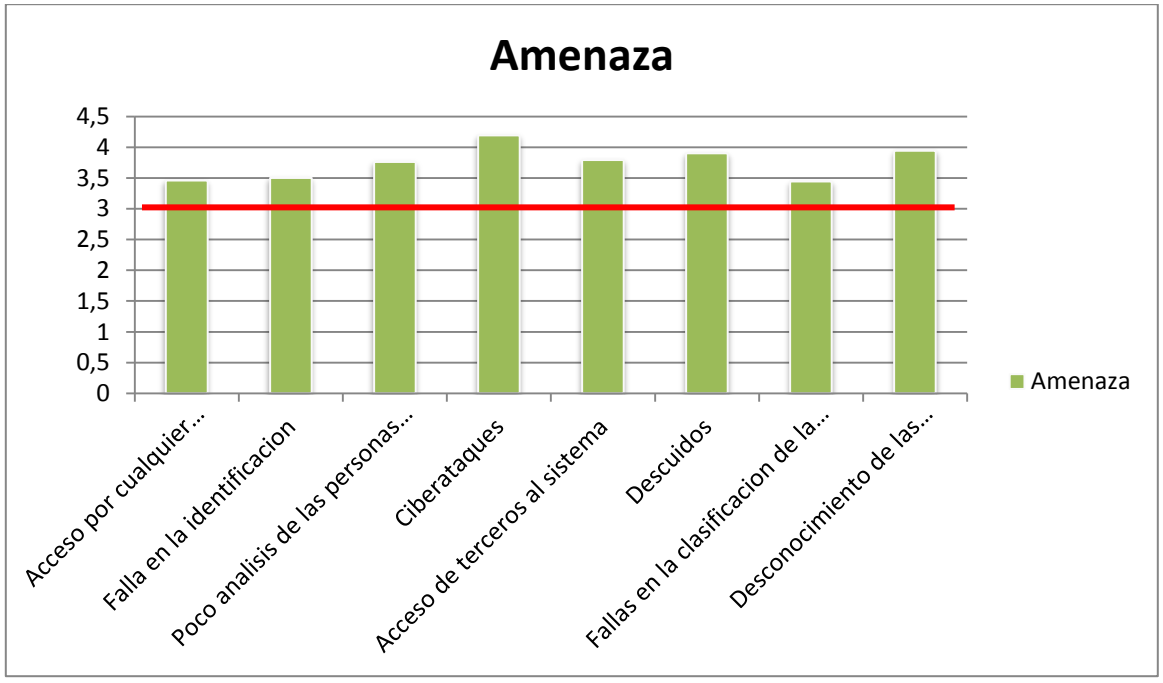
Si analizamos las medidas según el área en el que trabaja el personal podemos evaluar que tampoco existe una gran variación entre las medidas que aplican cada área. Un aspecto relevante a conocer es que en el caso de auditoria la mayor parte de los encuestados selecciono la opción de destrucción de papeles confidenciales mientras que en consultoría esa opción es la menos utilizada entre los encuestados.

Esto se debe a la diferencia de materiales que los mismos utilizan en su trabajo cotidiano.

3.5.2.4 Indique el grado de amenaza que representan las siguientes situaciones para la empresa

Con este tipo de pregunta queremos ver si los empleados cumplen con el promedio esperado para ver si conocen las amenazas a las que la empresa se enfrenta.

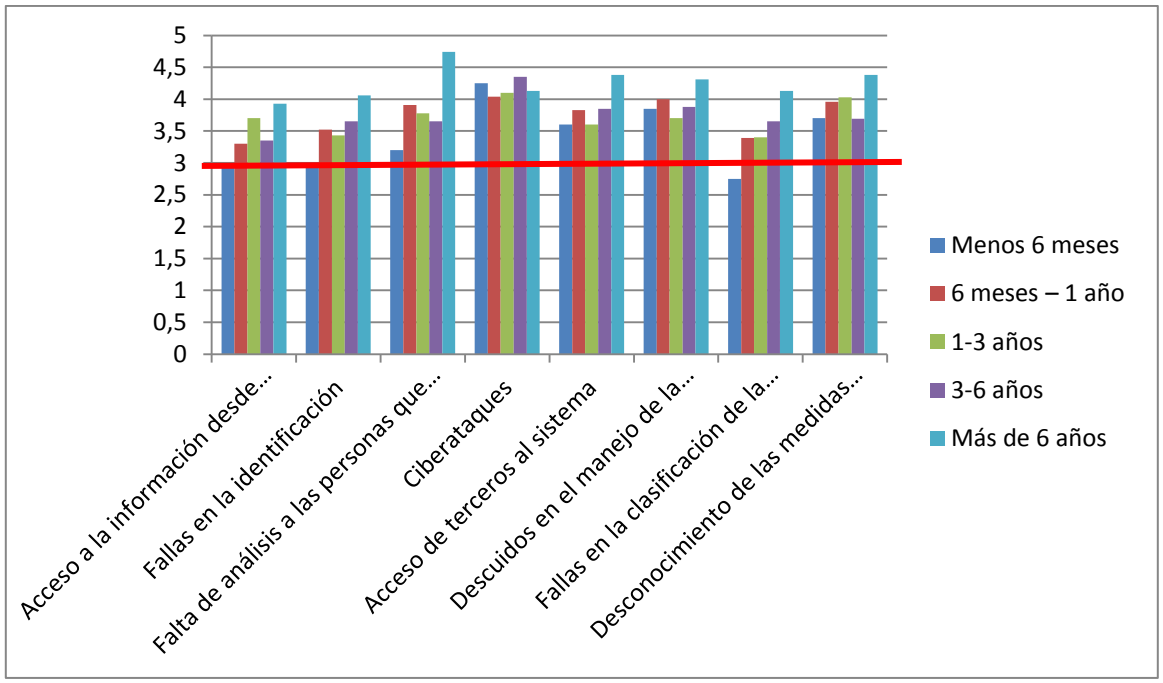
Amenaza	Empleados
Acceso a la información desde cualquier dispositivo	3,46
Fallas en la identificación	3,5
Falta de análisis a las personas que acceden	3,76
Ciberataques	4,19
Acceso de terceros al sistema	3,79
Descuidos en el manejo de la información	3,9
Fallas en la clasificación de la información	3,44
Desconocimiento de las medidas de seguridad	3,94



Todos los encuestados superaron la línea de corte que es 3. En este caso la respuesta es altamente positiva para nuestro estudio ya que este grado de respuesta nos permite entender que todos los empleados son conscientes de las amenazas a las que la empresa es susceptible.

En base a las respuestas obtenidas de los encuestados podemos decir que el ciberataque es para ellos la amenaza que más considera que la empresa puede sufrir mientras que la amenaza que menos consideran son las fallas en el momento de clasificar la información según el grado de sensibilidad que tiene el cliente hacia la misma.

Antigüedad / Amenaza	Menos 6 meses	6 meses a 1 año	1 a 3 años	3 a 6 años	Más de 6 años
Acceso a la información desde cualquier dispositivo	2,95	3,3	3,7	3,35	3,93
Fallas en la identificación	3	3,52	3,43	3,65	4,06
Falta de análisis a las personas que acceden	3,2	3,91	3,78	3,65	4,74
Ciberataques	4,25	4,04	4,1	4,35	4,13
Acceso de terceros al sistema	3,6	3,83	3,6	3,85	4,38
Descuidos en el manejo de la información	3,85	4	3,7	3,88	4,31
Fallas en la clasificación de la información	2,75	3,39	3,4	3,65	4,13
Desconocimiento de las medidas de seguridad	3,7	3,96	4,03	3,69	4,38



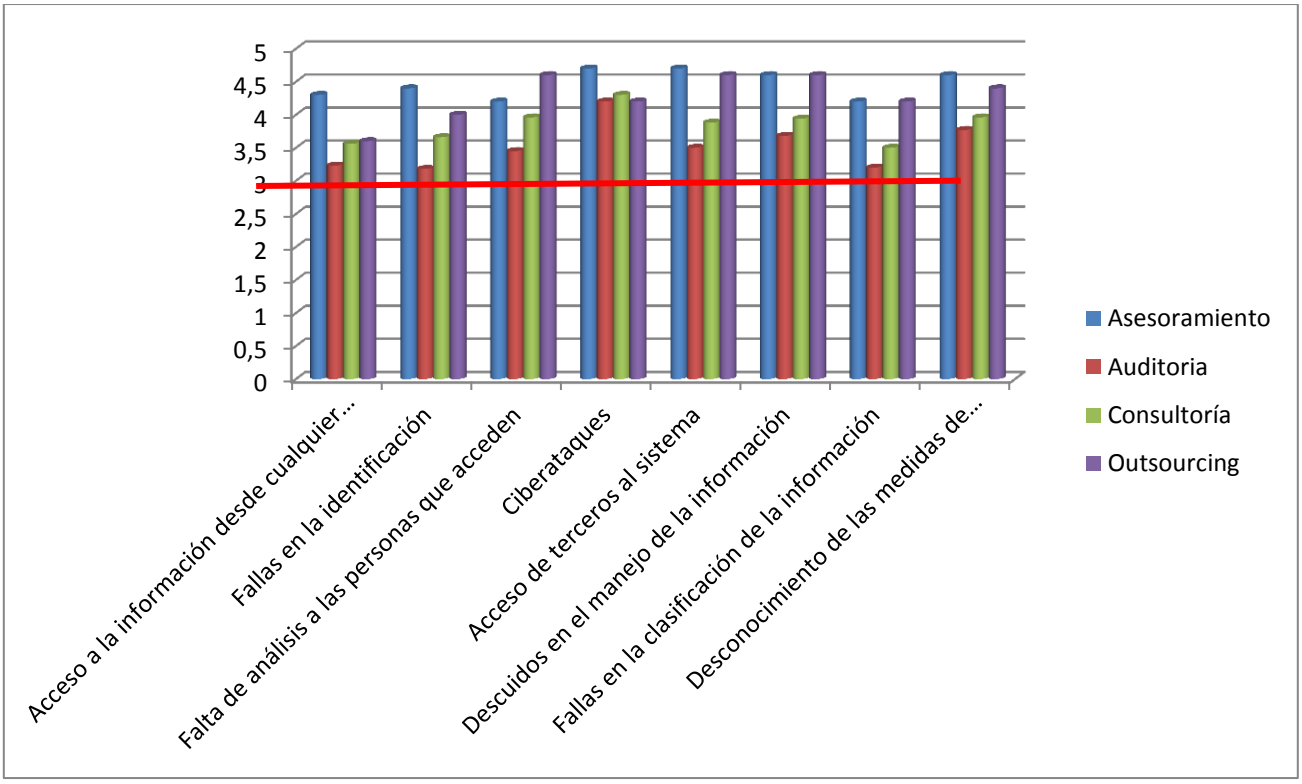
Si analizamos las respuestas en base a la antigüedad del personal podemos concluir lo siguiente las personas que tienen una antigüedad menor a los 6 meses consideran como la amenaza más fuerte los ciberataques mientras que la menos relevante es la falla en la clasificación de la información. Para el caso de la amenaza con mayor puntaje siempre se repiten los ciberataque excepto en el grupo del personal cuya antigüedad es mayor a 6 años que consideran como la mayor amenaza la falta de análisis en el permiso a las personas que acceden a la información.

Si analizamos la amenaza menos importante según los encuestados la misma varía según el grupo de edad ya que en los que poseen una antigüedad de entre 6 meses a 1 año es acceso a la información desde cualquier dispositivo móvil, para los que tienen uno a 3 años las fallas en la clasificación de la información y para los que tienen más de 6 años el acceso a la información desde cualquier dispositivo móvil

Un aspecto relevante es que si analizamos la dispersión entre el promedio más bajo y alto de cada segmento, el que está compuesto por personas con una antigüedad mayor a 6 años el promedio más bajo es de 3,93 lo cual significa que considera todas las amenazas nombradas muy importantes mientras que en el caso

cuya antigüedad es menor a 6 meses existen dos amenazas las cuales no logran superar la tasa de corte.

Área / Amenaza	Asesoramiento	Auditoria	Consultoría	Outsourcing
Acceso a la información desde cualquier dispositivo	4,3	3,23	3,56	3,6
Fallas en la identificación	4,4	3,18	3,66	4
Falta de análisis a las personas que acceden	4,2	3,45	3,96	4,6
Ciberataques	4,7	4,2	4,3	4,2
Acceso de terceros al sistema	4,7	3,5	3,88	4,6
Descuidos en el manejo de la información	4,6	3,68	3,94	4,6
Fallas en la clasificación de la información	4,2	3,2	3,5	4,2
Desconocimiento de las medidas de seguridad	4,6	3,77	3,96	4,4

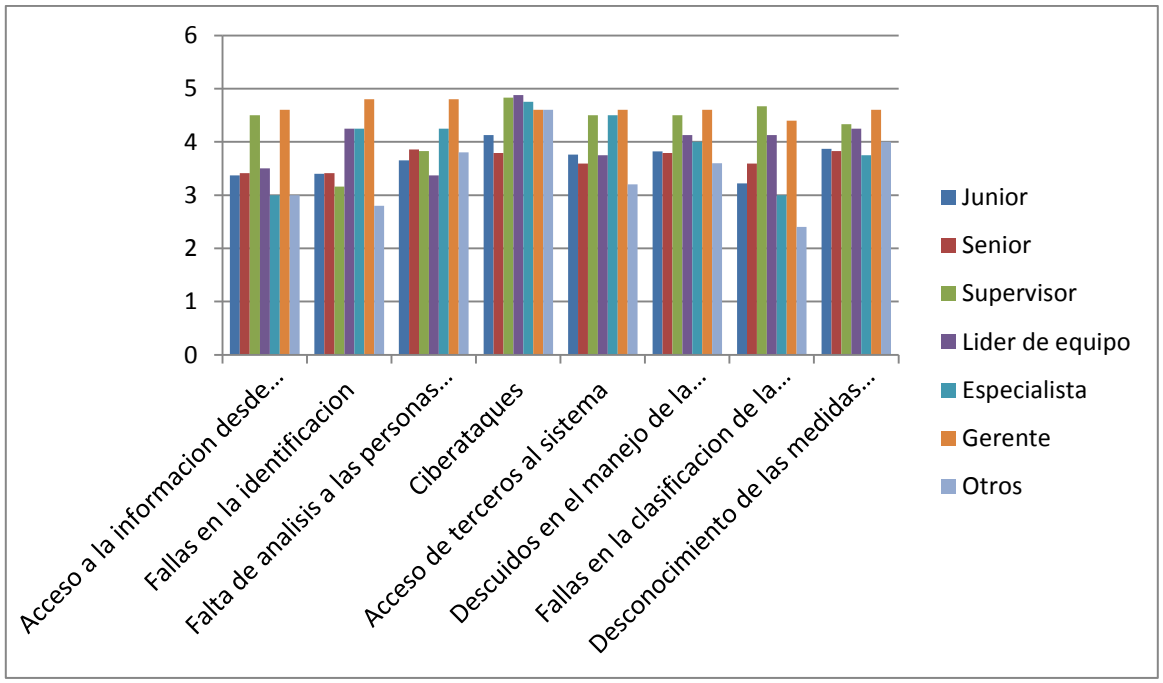


Si analizamos las amenazas según el área podemos notar que todas tienen sus promedios por encima de la tasa de corte. Sin embargo, auditoría y consultoría que

son poseen más cerca de la tasa de corte dado que las mayorías de las opciones según los empleados del área de asesoramiento y Outsourcing tienen su promedio por encima de los 4 puntos.

Este aspecto se debería analizar con un criterio sumamente objetivo ya que auditoría y consultoría manejan información relevante y altamente sensible para el cliente por lo que se podría entender como que en determinadas áreas descuidan posibles riesgos latentes.

Amenaza	Junior	Senior	Supervisor	Líder de equipo	Especialista	Gerente	Otros
Acceso a la información desde cualquier dispositivo	3,37	3,41	4,5	3,5	3	4,6	3
Fallas en la identificación	3,4	3,41	3,16	4,25	4,25	4,8	2,8
Falta de análisis a las personas que acceden	3,65	3,86	3,83	3,37	4,25	4,8	3,8
Ciberataques	4,13	3,79	4,83	4,88	4,75	4,6	4,6
Acceso de terceros al sistema	3,76	3,59	4,5	3,75	4,5	4,6	3,2
Descuidos en el manejo de la información	3,82	3,79	4,5	4,13	4	4,6	3,6
Fallas en la clasificación de la información	3,22	3,59	4,67	4,13	3	4,4	2,4
Desconocimiento de las medidas de seguridad	3,87	3,83	4,33	4,25	3,75	4,6	4



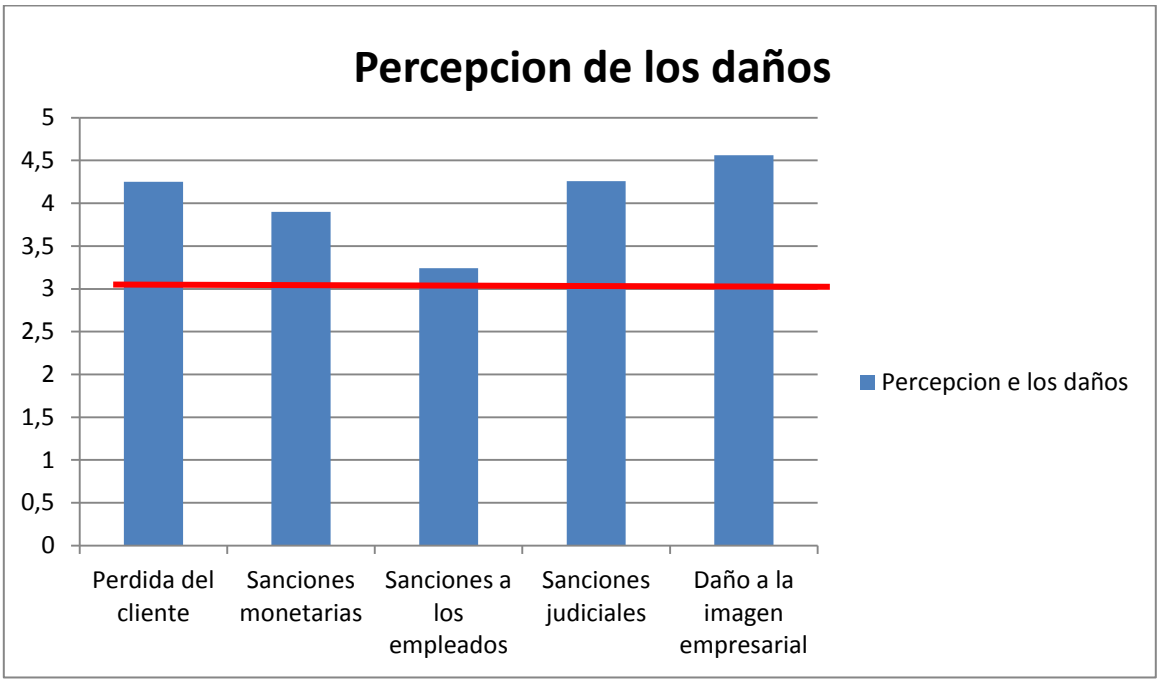
Analizando por puesto podemos ver que en todos los casos se supera la tasa de corte (3) excepto en los puestos de técnicos, pasantes y jóvenes profesionales esto se puede justificar considerando que son empleados los cuales están poco tiempo en su puesto y sus responsabilidades son limitadas y altamente controladas por sus superiores.

En el caso de los gerentes vemos le indicaron a las amenazas un promedio superior al resto de los distintos puestos.

3.5.2.5 Indique el grado de daño que pueden representar las siguientes situaciones para la empresa

El objetivo que perseguimos con este tipo de cuestionamiento es ver que concepción tienen los empleados de la empresa sobre las posibles consecuencias que puede tener una fuga de información.

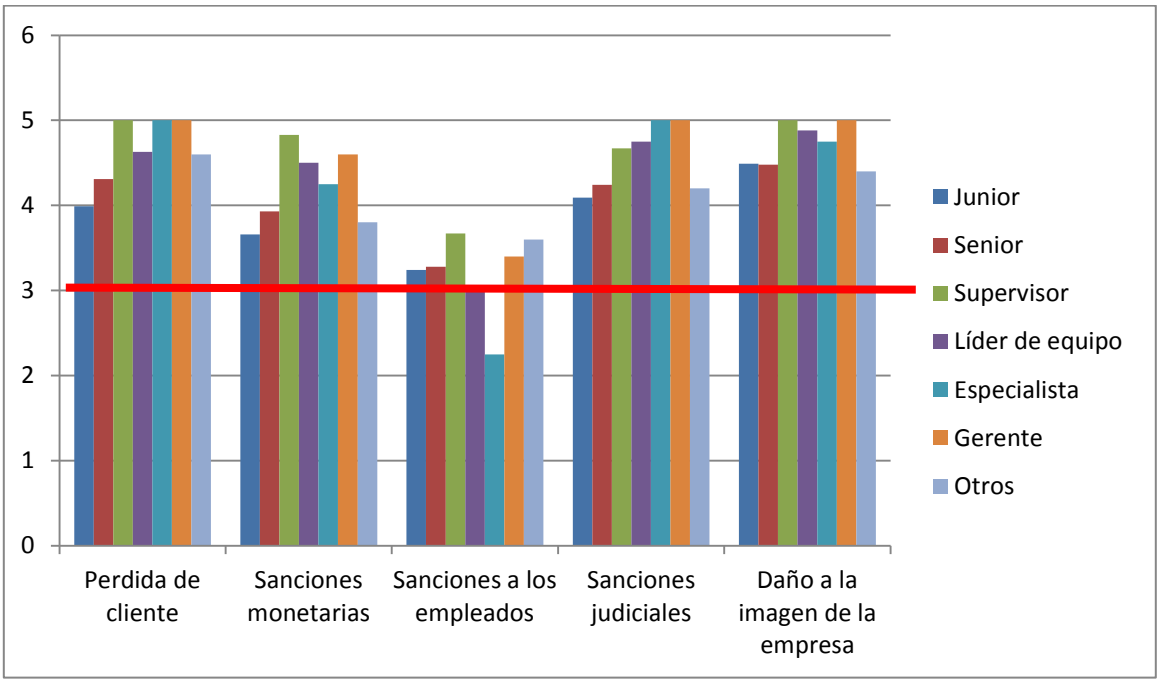
Daños	SI
Perdida de cliente	4,25
Sanciones monetarias	3,9
Sanciones a los empleados	3,24
Sanciones judiciales	4,26
Daño a la imagen de la empresa	4,56



Para el caso de percepción de daños la tasa de corte es de 3. Para nuestro agrado podemos ver que las consecuencias como la pérdida del cliente, sanciones judiciales y daño a la imagen de la empresa son las que poseen un promedio mayor que el resto de las opciones.

Las sanciones a los empleados está más cerca de la tasa de corte lo cual es preocupante ya que en la mayoría los casos que existe una fuga de información la primera medida llevada a cabo es desvincular al empleado de la empresa.

Puesto / Daño	Junior	Senior	Supervisor	Líder de equipo	Especialista	Gerente	Otros
Perdida de cliente	3,99	4,31	5	4,63	5	5	4,6
Sanciones monetarias	3,66	3,93	4,83	4,5	4,25	4,6	3,8
Sanciones a los empleados	3,24	3,28	3,67	3	2,25	3,4	3,6
Sanciones judiciales	4,09	4,24	4,67	4,75	5	5	4,2
Daño a la imagen de la empresa	4,49	4,48	5	4,88	4,75	5	4,4



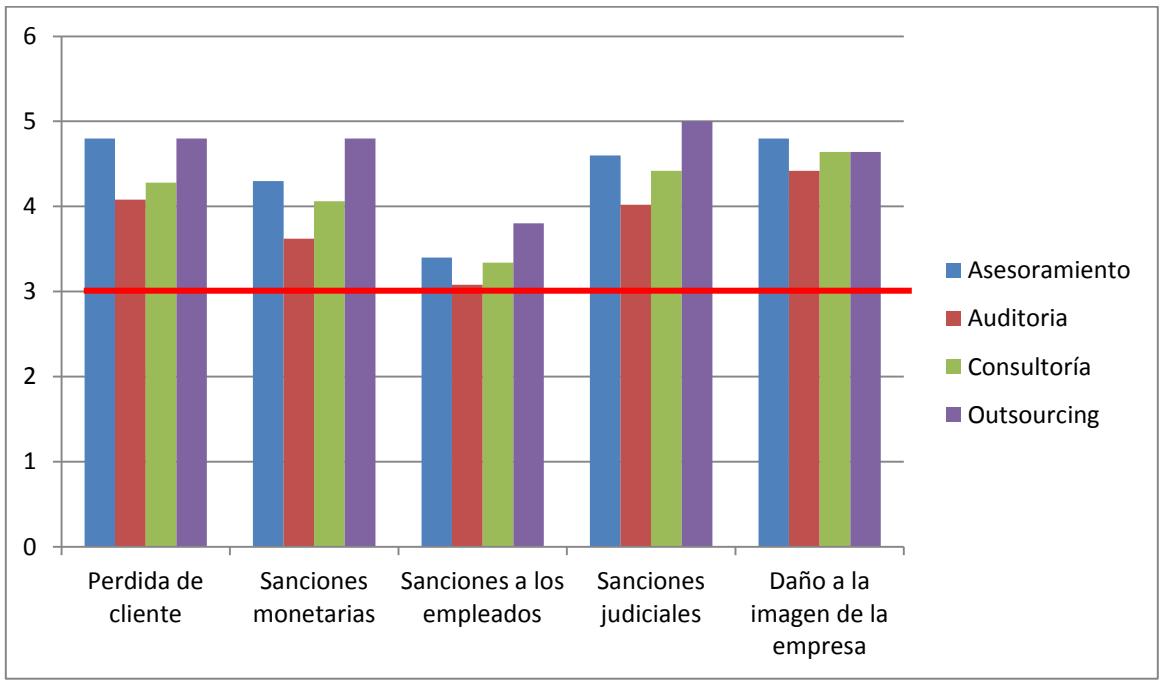
Si evaluamos como consideran el daño los empleados según el puesto podemos ver que solo en el caso de los especialistas la consecuencia sanciones a los empleados no llega a superar la tasa de corte (2,25<3). Después si analizamos para cada puesto en particular podemos ver que en la mayoría existe un promedio bastante parejo excepto en el caso de los especialistas y los gerentes.

Un aspecto a considerar es que para el caso de pérdida de los clientes todos los encuestados que son supervisores, especialistas o gerentes lo consideraron el daño más importante. Sucede lo mismo para el caso de sanciones judiciales pero en estos casos los especialistas y gerentes consideran eso. En el caso del daño de la

empresa los supervisores y gerentes consideran que son las consecuencias más importantes.

A su vez, si analizamos las respuestas de los gerentes estos consideran la mayoría de las consecuencias generaran un daño irreversible para la empresa.

Área / Daño	Asesoramiento	Auditoria	Consultoría	Outsourcing
Perdida de cliente	4,8	4,08	4,28	4,8
Sanciones monetarias	4,3	3,62	4,06	4,8
Sanciones a los empleados	3,4	3,08	3,34	3,8
Sanciones judiciales	4,6	4,02	4,42	5
Daño a la imagen de la empresa	4,8	4,42	4,64	5



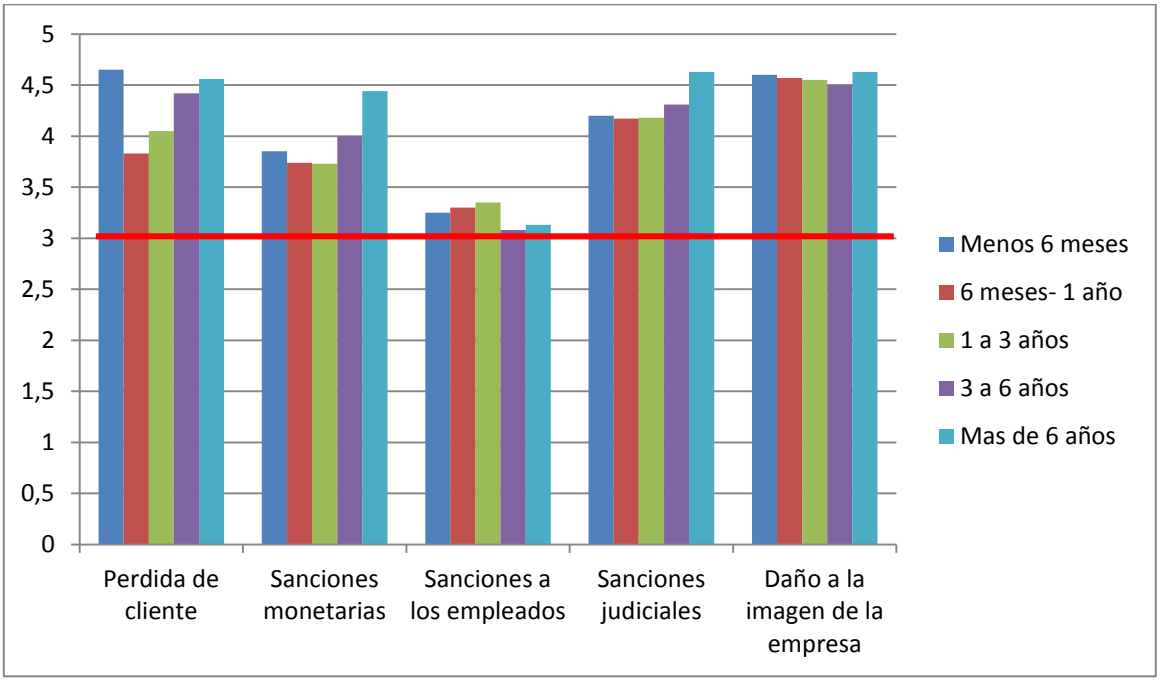
En cada área las percepciones de las consecuencias ante una fuga de información son totalmente distintas. En todos los casos los promedios superan la tasa de corte sin embargo tanta dispersión es compleja ya que podemos analizar que el hecho de que los empleados no sean conscientes de que pueden ser sancionados no los hace tomar conciencia de que si son responsables de una fuga de información están

expuestos a una sanción ya sea judicial y obviamente terminar su relación contractual con la empresa.

El área que le otorgo mayor complejidad para la empresa fue Outsourcing y la que

Antigüedad / Daño	Menos 6 meses	6 meses a 1 año	1 a 3 años	3 a 6 años	Más de 6 años
Perdida de cliente	4,65	3,83	4,05	4,42	4,56
Sanciones monetarias	3,85	3,74	3,73	4	4,44
Sanciones a los empleados	3,25	3,3	3,35	3,08	3,13
Sanciones judiciales	4,2	4,17	4,18	4,31	4,63
Daño a la imagen de la empresa	4,6	4,57	4,55	4,5	4,63

menos consciente es de estos daños es auditoria.



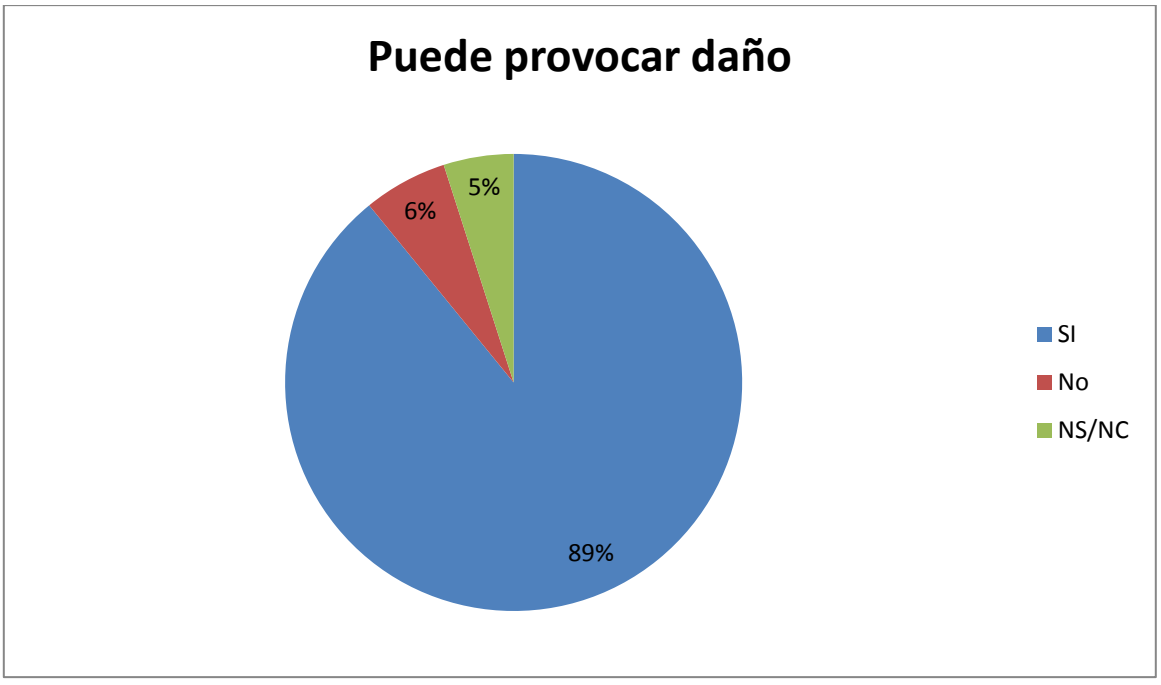
A favor de las empresas, este análisis demuestra que por más que existan empleados cuya antigüedad no logre superar los seis meses en ningún caso ninguna opción estuvo por debajo de la tasa de corte, inclusive se puede decir que tuvieron una consideración bastante similar al resto de los empleados con mayor antigüedad.

Igualmente podemos ver que en los casos de una antigüedad de entre 6 meses y 3 años tienen una consideración mucho menor que el resto de los empleados por lo que sería necesario realizar una capacitación para lograr que mejore su concepto de los daños.

3.5.2.6 Considera que de no respetar alguna norma de seguridad podría tener como consecuencia una fuga de información

Con este tipo de interrogante se busca analizar cuál es el grado de conciencia que tienen los empleados considerando que si no cumplen con las normativas si habría una fuga de información.

	Empleados	%
Si	112	90%
No	7	6%
NS/NC	6	4%

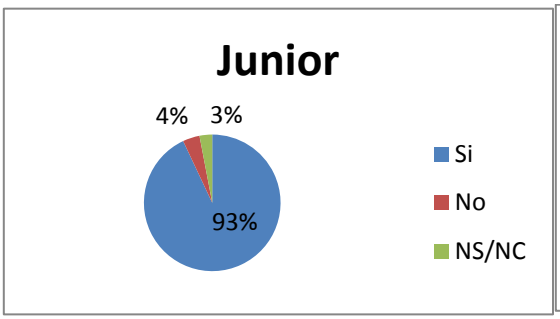


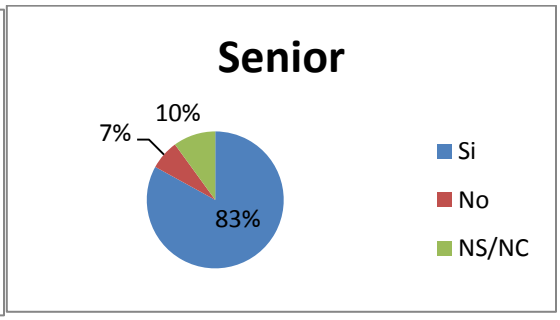
Al consultarle a los empleados si consideran que al no respetar las medidas de seguridad determinadas por la gerencia están poniendo en riesgo a la empresa ante una fuga de información el 90% dijo que si, mientras que el 6% que no. Existe un 4%

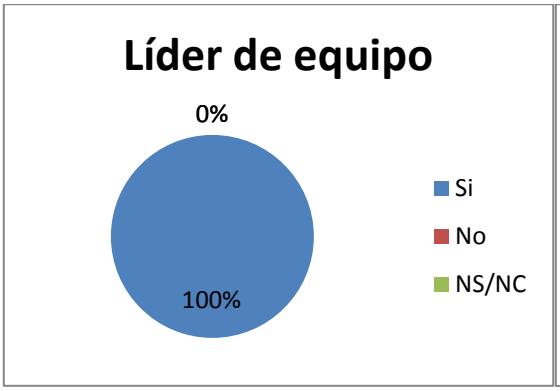
que no sabe las consecuencias que pueden tener no cumplir con las normas de seguridad.

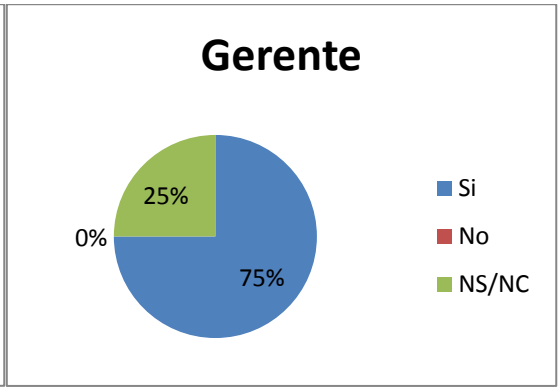
El porcentaje que dijo que si es sumamente alto y permite asegurar que los empleados son conscientes de que su papel es fundamental para resguardar la información.

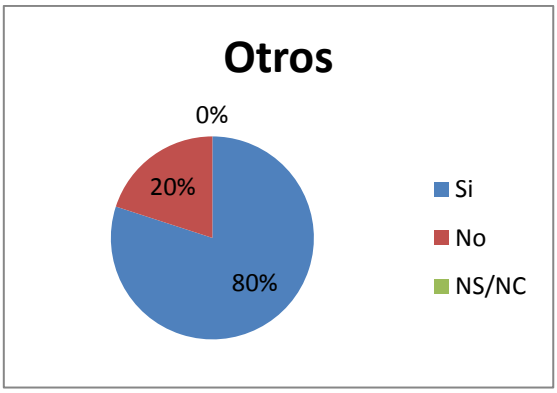
Puesto	Junior		Senior		Supervisor		Líder de equipo		Especialista		Gerente		Otros	
Si	64	93%	24	83%	5	83%	8	100%	4	100%	3	75%	4	80%
No	3	4%	2	7%	1	17%	0	0%	0	0%	0	0%	1	20%
NS/NC	2	3%	3	10%	0	0%	0	0%	0	0%	1	25%	0	0%

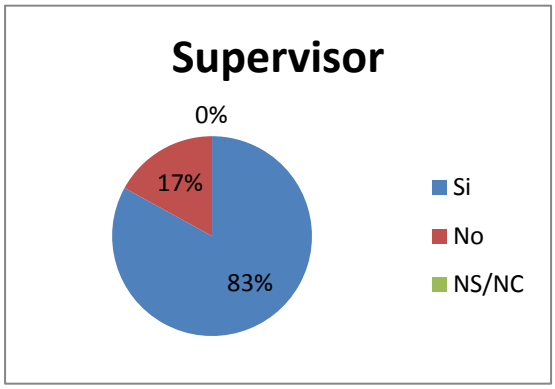






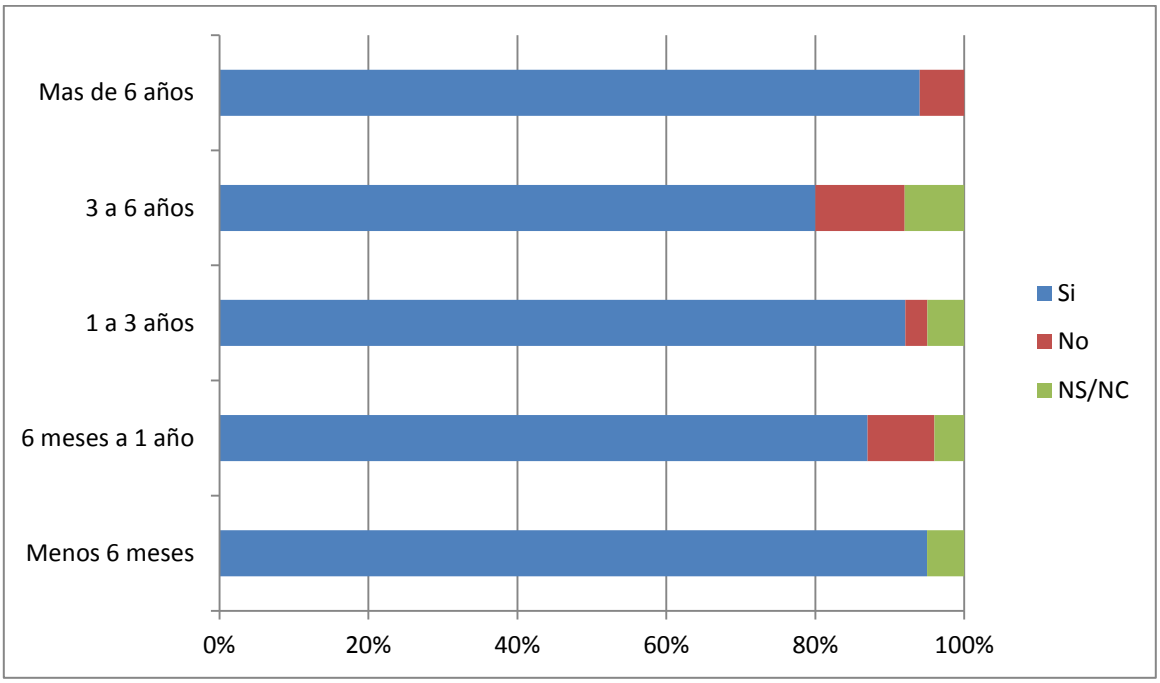






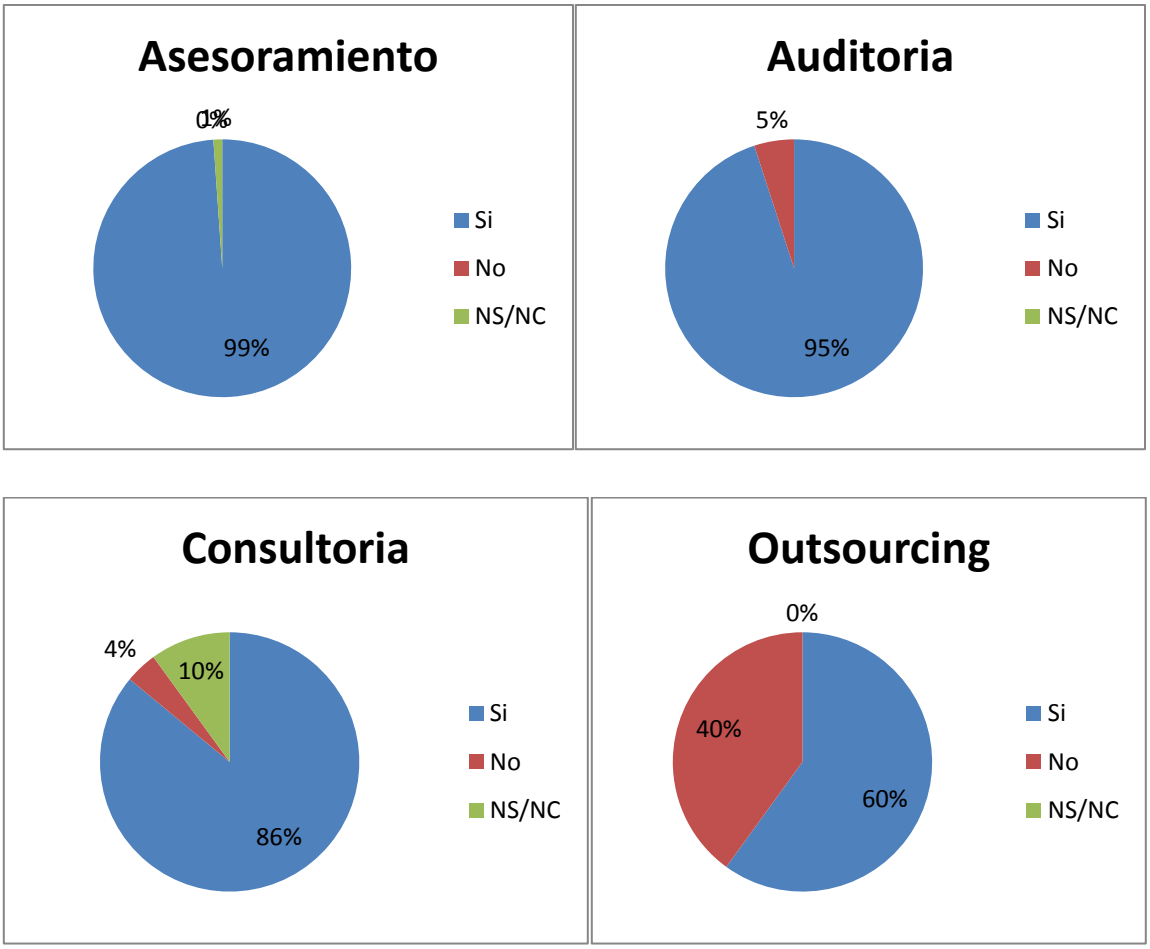
Al analizar la conciencia ante sus actos según el puesto que ocupa podemos notar que en el caso que hay más dudas es en los jóvenes profesionales, pasantes y técnicos. Podemos evaluar que la capacitación en los juniors y seniors ha generado el suficiente conocimiento para que ellos determinen cuales son las consecuencias que tendrá incumplir con las medidas determinadas por la gerencia de seguridad. En el caso de líderes de equipos y especialistas el porcentaje de que consideran que exponen a la empresa a un riesgo es del 100%.

Antigüedad	Menos 6 meses		6 meses a 1 año		1 a 3 años		3 a 6 años		Más de 6 años	
Si	19	95%	20	87%	37	93%	21	80%	15	94%
No	0	0%	2	9%	1	3%	3	12%	1	6%
NS/NC	1	5%	1	4%	2	5%	2	8%	0	0%



Consideramos que este tipo de respuesta debe ser analizada según la antigüedad que tiene el personal en la empresa ya que a medida que van creciendo en la compañía han participado en gran cantidad de cursos de capacitación por ende tendrán una mayor conciencia de las políticas implementadas por la empresa. En este caso podemos evaluar que existen ciertas falencias en los empleados de entre 6 meses a un año y de 3 años a 6 ya que el porcentaje que considera que expone a la empresa a una fuga por no cumplir con las medidas es menor al 90%.

Área	Asesoramiento		Auditoria		Consultoría		Outsourcing	
Si	9	90%	57	95%	43	86%	3	60%
No	0	0%	3	5%	2	4%	2	40%
NS/NC	1	10%	0	0%	5	10%	0	0%

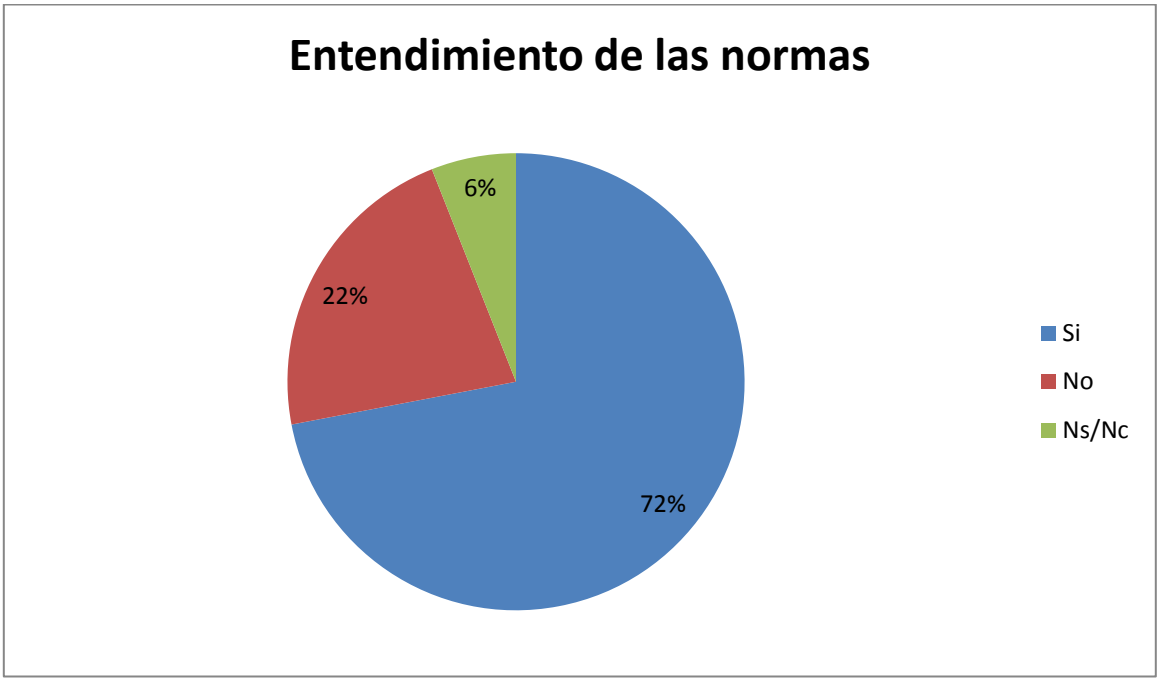


Al analizar las respuestas según el área donde trabajan, los resultados más preocupantes se dan en el área de consultoría ya que un 10% de los encuestados contestaron que no saben si un incumplimiento de las medidas de seguridad expone a la empresa ante distintos riesgos. Al igual que el área de Outsourcing que un 20% contesto que no considera que expone a la empresa a ningún riesgo. El resto de las áreas contestaron 90% y 95% que si consideran que exponen a la empresa al riesgo de fuga de información.

3.5.2.7 Considera que usted conoce y entiende todas las normas de seguridad de la información que se aplican a la empresa

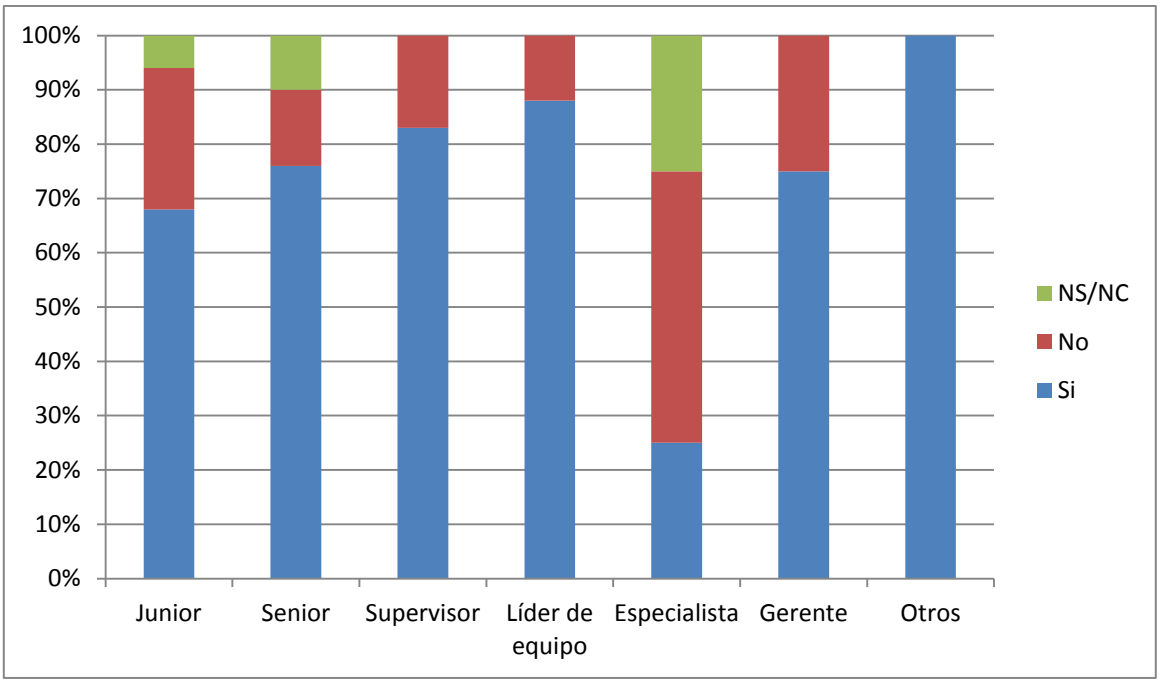
En este tipo de cuestión se busca analizar no solo si el empleados aplica las normas de seguridad impuesta por la empresa sino que si las entiende.

	Empleados	%
Si	90	72%
No	27	22%
NS/NC	8	6%



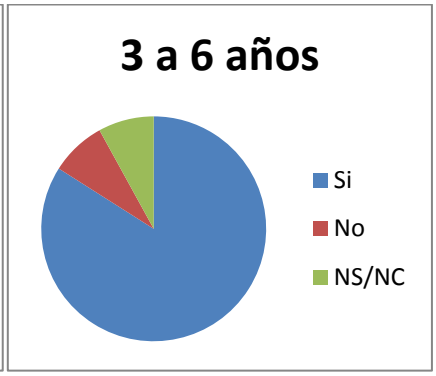
Al consultarles a los empleados si entienden las normas de seguridad aplicadas el 72% considera que si mientras que el 22% que no. Existe un 6% que no sabe si las entiende sino que las aplica porque así lo determina la empresa.

Puesto	Junior		Senior		Supervisor		Líder de equipo		Especialista		Gerente		Otros	
Si	47	68%	22	76%	5	83%	7	88%	1	25%	3	75%	5	100%
No	18	26%	4	14%	1	17%	1	12%	2	50%	1	25%	0	0%
NS/NC	4	6%	3	10%	0	0%	0	0%	1	25%	0	0%	0	0%



Al analizar las respuestas en base al puesto que los empleados ocupan notamos que hay una falla de entendimiento en especial en los junior y especialistas. Esto es probable porque son personas que recién se inician en la empresa y aún no han llegado a cumplir con los planes de capacitaciones.

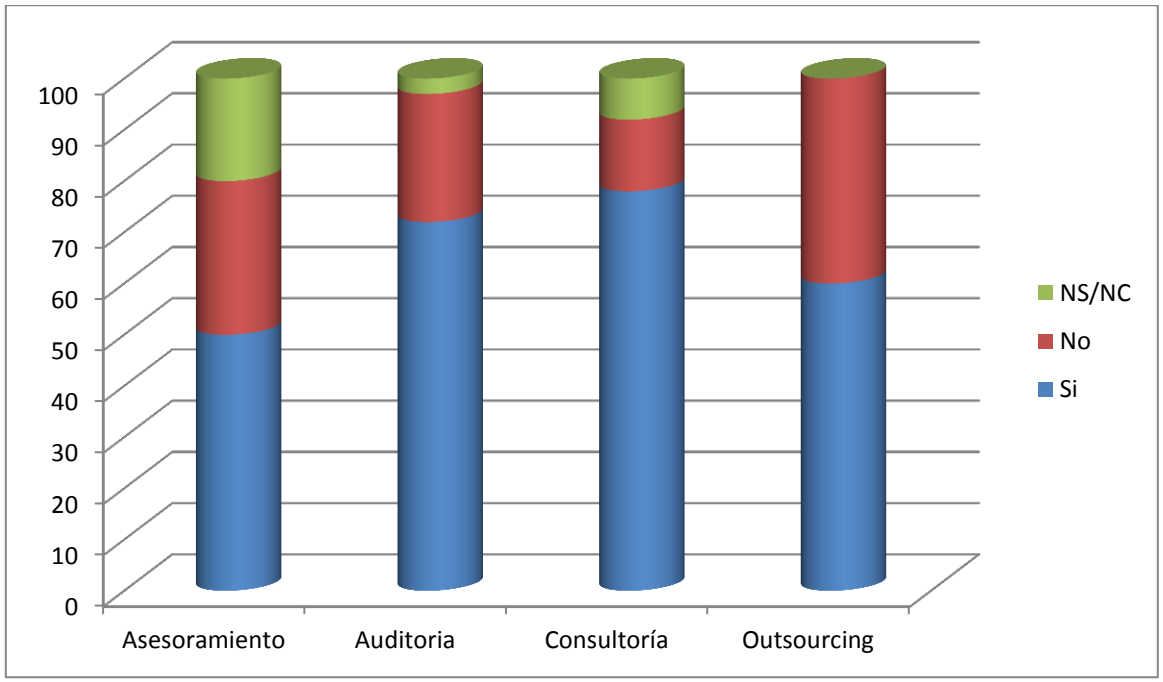
Antigüedad	Menos de 6 meses		6 meses a 1 año		1 a 3 años		3 a 6 años		Más de 6 años	
Si	15	75%	15	65%	28	70%	22	84%	10	94%
No	2	10%	7	31%	11	28%	2	8%	5	6%
NS/NC	3	15%	1	4%	1	2%	2	8%	1	0%



Al analizar las respuestas por antigüedad podemos ver que en el caso de los que tienen menos de 6 meses en la empresa contestaron un 75% que sí, los que llevan trabajando entre 6 meses a 1 año el 65%. Y después el porcentaje empieza a aumentar a medida que aumenta el tiempo de permanencia en la empresa.

Un indicador a destacar es que existe un gran porcentaje de desconocimiento en los que llevan trabajando menos de 6 meses y entre 3 a 6 años.

Área	Asesoramiento		Auditoria		Consultoría		Outsourcing	
Si	5	50%	43	72%	39	78%	3	60%
No	3	30%	15	25%	7	14%	2	40%
NS/NC	2	20%	2	3%	4	8%	0	0%

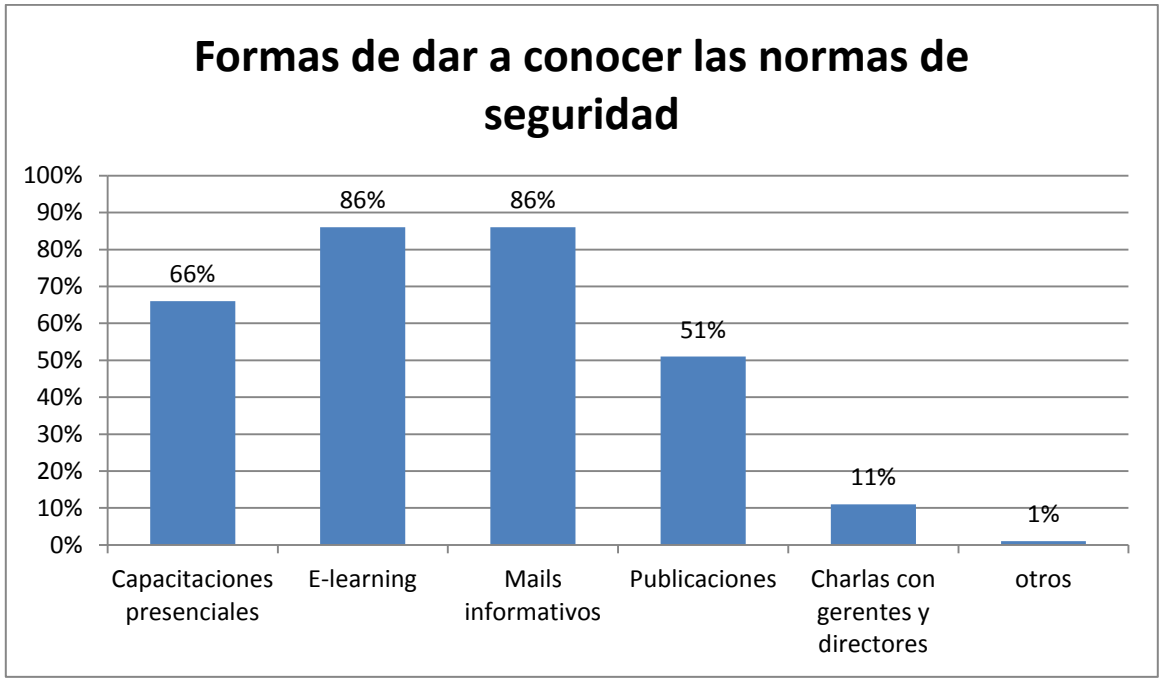


Cuando se ven las respuestas por área es un indicador preocupante ya que en ninguna de las áreas se logra el entendimiento del 80% esto es un indicador grave ya que implica que los empleados solo hacen lo que se les dice y al no entender el por qué se hace eso tampoco pueden aportar ideas para lograr un mejor sistema. Exceptuando el área de Outsourcing todas las demás áreas poseen empleados que no pueden indicar si entienden o no las medidas operativas que llevan a cabo en sus actividades diarias.

3.5.2.8 Forma en la que se le dan a conocer a usted las normas de seguridad de la información aplicadas

Lo que buscamos con este tipo de interrogante es ver qué forma tienen las empresas para darle a conocer a sus empleados las normas de seguridad.

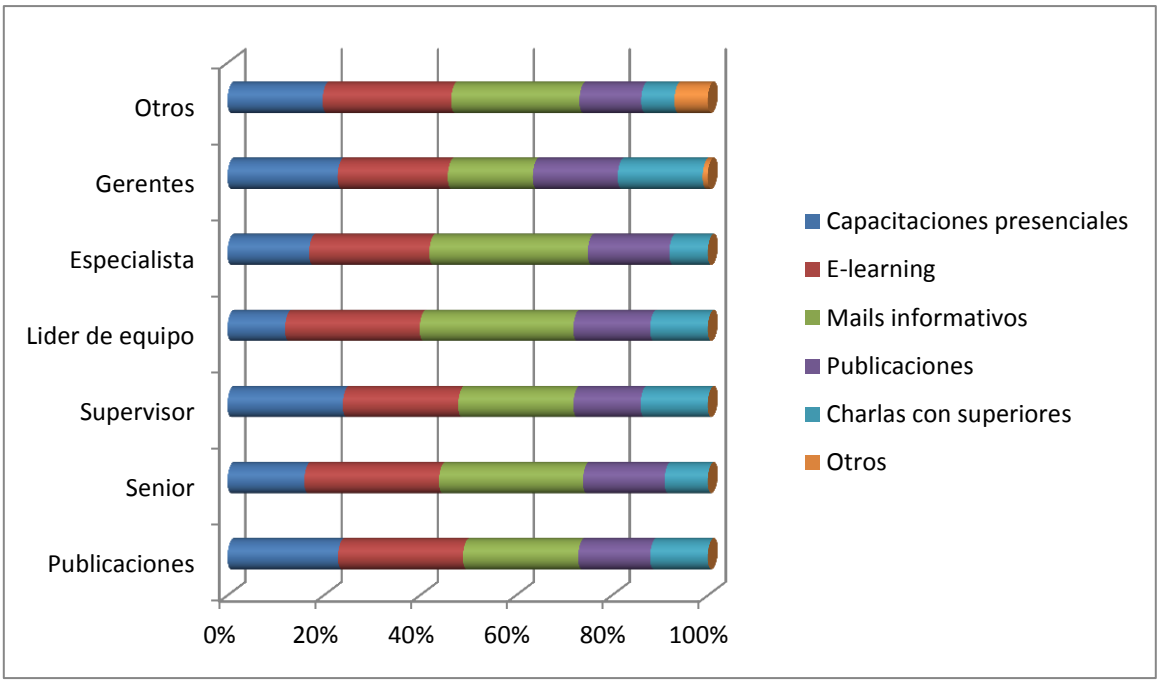
Formas de dar a conocer	Empleados	%
Capacitación presencial	83	66%
E-learning	107	86%
Mails Informativos	107	86%
Publicaciones de la empresa	64	51%
Charlas con gerentes/directores	48	11%
Otros	2	1%



Al consultarle a los empleados de que forma la empresa les permite conocer las normas de seguridad las medidas más mencionadas fueron E-learnings y mails informativos cada una obtuvo un 86% mientras que la forma que menos se aplica son

charlas con gerentes o directores que solo el 11% de los encuestados confirmo que tiene esa posibilidad en su empresa.

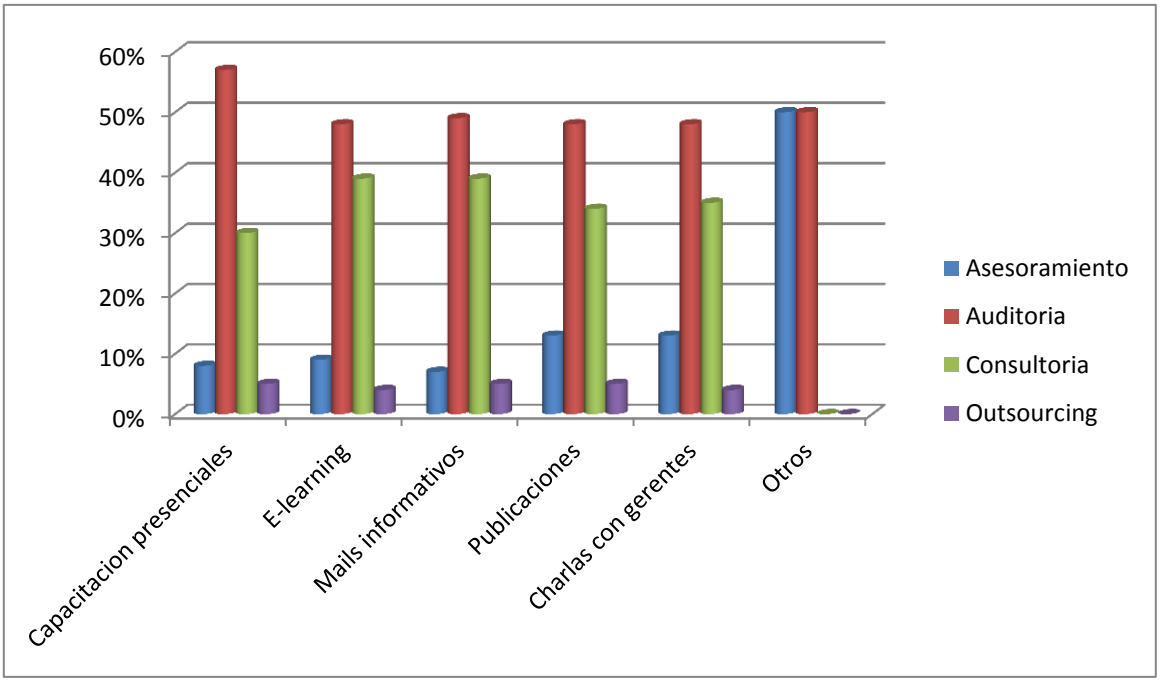
Formas de dar a conocer	Junior		Senior		Supervisor		Líder de equipo		Especialista		Gerente		Otros	
Capacitacion presencial	51	23%	14	16%	5	24%	3	12%	2	17%	5	22%	3	20%
E-learning	58	26%	25	28%	5	24%	7	28%	3	25%	5	22%	4	27%
Mails Informativos	55	24%	27	30%	5	24%	8	32%	4	33%	4	17%	4	27%
Publicaciones de la empresa	34	15%	15	17%	3	14%	4	16%	2	17%	4	17%	2	13%
Charlas con gerentes/directores	28	12%	8	9%	3	14%	3	12%	1	8%	4	17%	1	7%
Otros	0	0%	0	0%	0	0%	0	0%	0	0%	1	4%	1	7%



Las formas para dar a conocer varían ampliamente según el puesto que ocupan el personal ya que en el caso de los juniors la forma mas mencionada son los e-

learnings (26%), mientras que para los seniors, lideres de equipos y especialistas son los mails informativos con un 30%, 24% y 32% respectivamente. En el caso de los supervisores esta pude variar entre capacitaciones presenciales, E-learnings y mails informativos. En el caso de los gerentes las formas son capacitaciones presenciales y E-learnings.

Formas de dar a conocer	Menos 6 meses		6 meses a 1 año		1 a 3 años		3 a 6 años		Más de 6 años	
Capacitación presencial	16	19%	15	18%	28	34%	12	14%	12	14%
E-learning	18	17%	22	21%	31	29%	21	20%	15	14%
Mails Informativos	17	16%	16	15%	36	34%	24	22%	14	13%
Publicaciones de la empresa	10	16%	12	19%	21	33%	10	16%	12	19%
Charlas con gerentes/directores	5	10%	8	17%	18	38%	6	13%	11	23%
Otros	0	0%	0	0%	0	0%	1	50%	1	50%



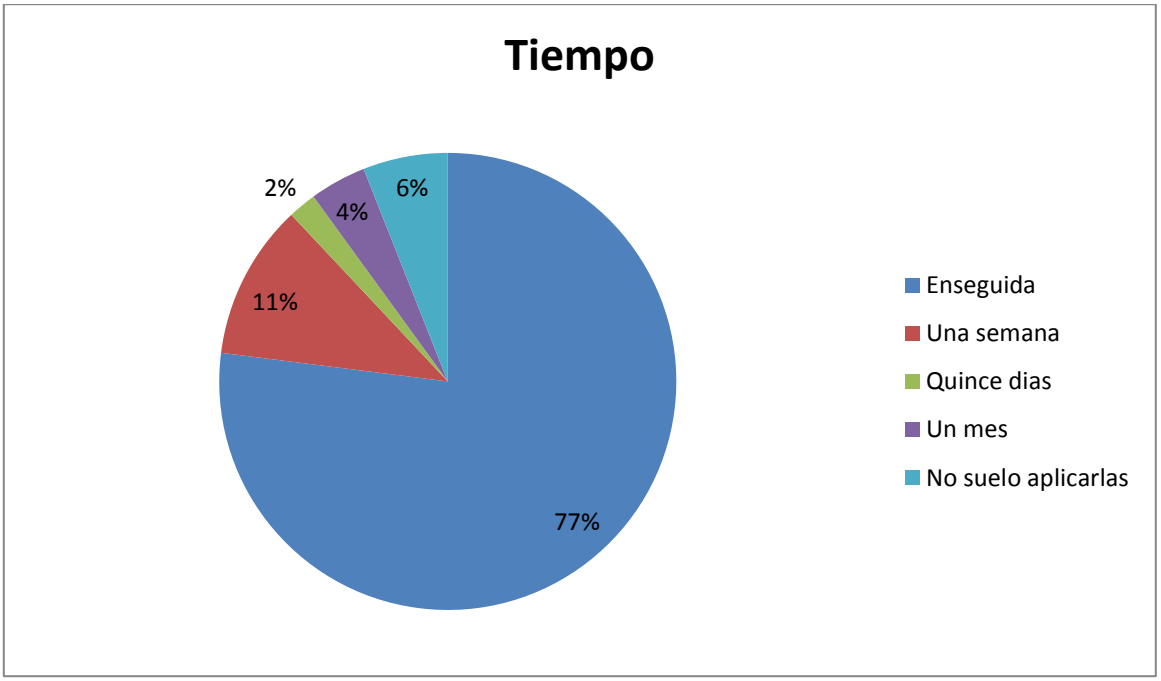
Para el área de asesoramiento la forma más utilizada son los congresos mientras que en auditoria son las publicaciones internacionales. Para el área de consultoría se utilizan los e-learnings y mails informativos como formas de capacitar al empleado y

en Outsourcing las formas más utilizadas son mails informativos y publicaciones de la empresa.

3.5.2.9 Tiempo que le lleva adoptar las normas de seguridad una vez que se las comunicaron

En esta pregunta buscamos ver la efectividad que tienen los planes de capacitaciones sobre los empleados.

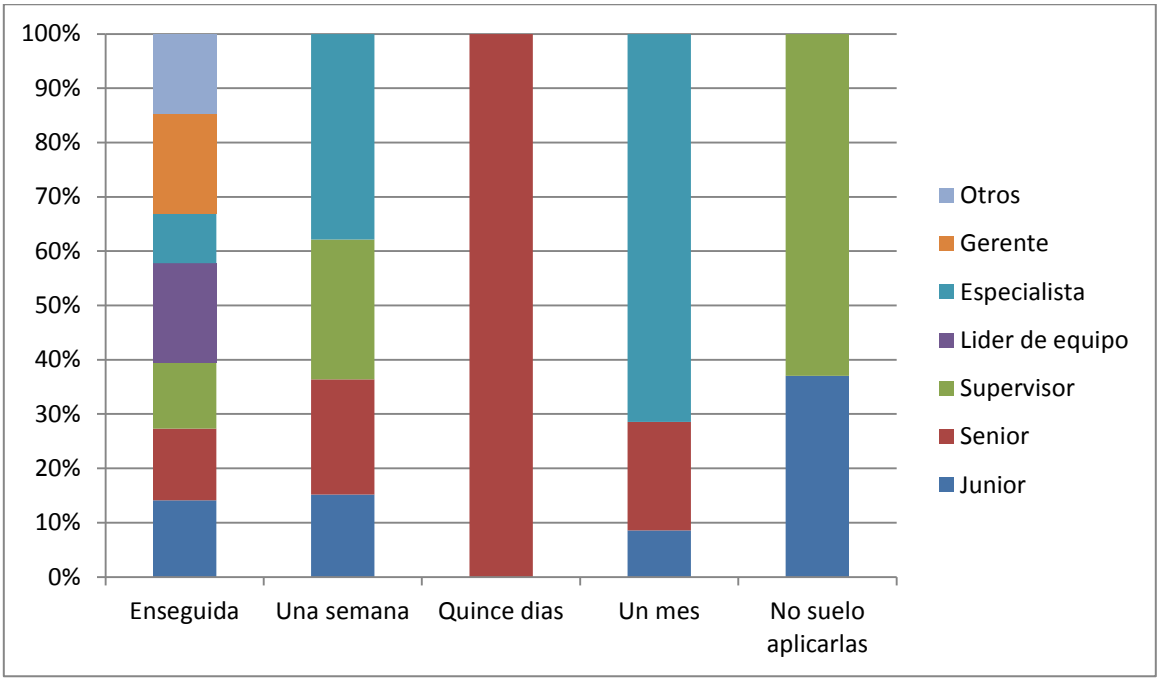
Tiempo	Empleados	%
Enseguida las aplico	96	77%
Una semana	14	11%
Quince días	2	2%
Un mes	5	4%
No suelo aplicarlas	8	6%



Al consultarles a los encuestados cuanto tiempo le lleva adquirir como propias las nuevas medidas que establece la gerencia el 77% contesto que enseguida las aplica mientras que el 11% tarda una semana. Hay un 12% que le lleva más tiempo entre

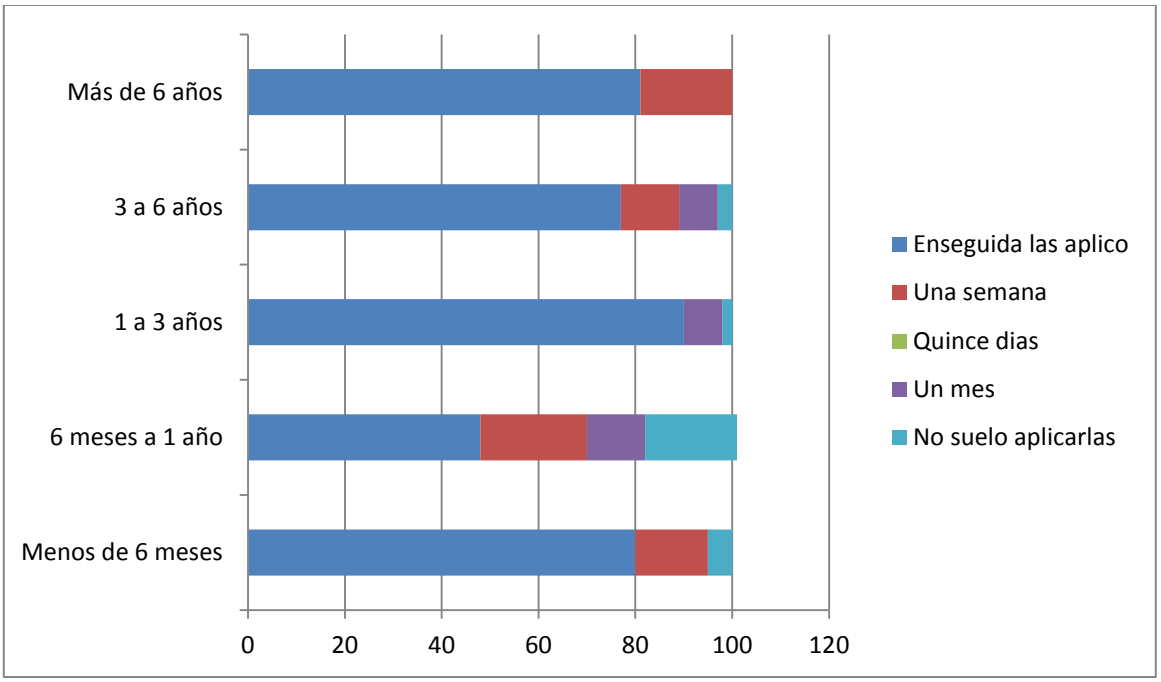
ellos están los que tardan quince días que son el 2% de los encuestados, un mes 4% y hubo un grupo que dijo que no suele aplicarlas que representa el 6%.

Tiempo	Junior		Senior		Supervisor		Líder de equipo		Especialista		Gerente		Otros	
Enseguida las aplico	53	77%	21	72%	4	66%	8	100%	2	50%	4	100%	4	80%
Una semana	7	10%	4	14%	1	17%	0	0%	1	25%	0	0%	1	20%
Quince días	0	0%	2	7%	0	0%	0	0%	0	0%	0	0%	0	0%
Un mes	2	3%	2	7%	0	0%	0	0%	1	25%	0	0%	0	0%
No suelo aplicarlas	7	10%	0	0%	1	17%	0	0%	0	0%	0	0%	0	0%



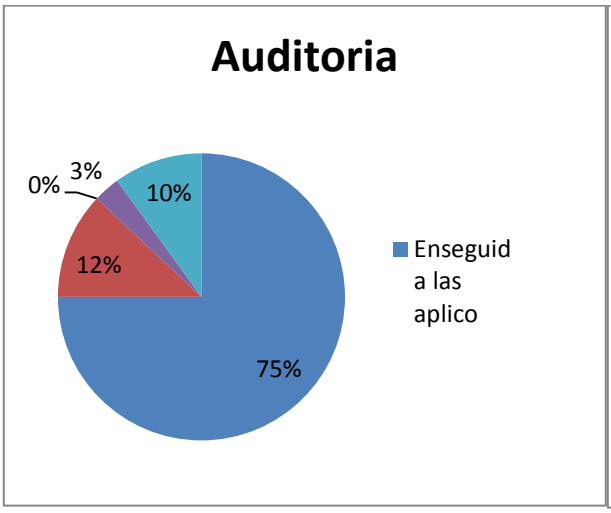
Si analizamos las respuestas en base al puesto jerárquico que ocupan en la empresa podemos ver que a medida que ascienden el tiempo que les toma aplica las medidas es mucho menor. Consideramos que este es un aspecto que la empresa debe analizar ya que deben reforzar en los puestos de menor seniority el hecho de porque son importantes que implementen a la brevedad las nuevas medidas.

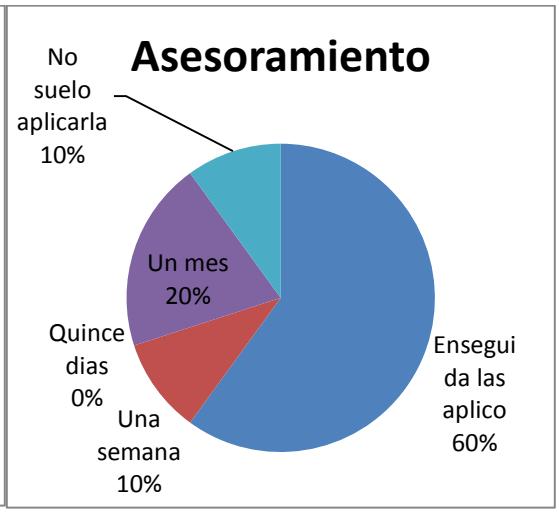
Puesto	Menos de 6 meses		6 meses a 1 año		1 a 3 años		3 a 6 años		Más de 6 años	
Enseguida las aplico	16	80%	11	48%	36	90%	20	77%	13	81%
Una semana	3	15%	5	22%	0	0%	3	12%	3	19%
Quince días	0	0%	2	9%	0	0%	0	0%	0	0%
Un mes	0	0%	2	9%	1	2%	2	8%	0	0%
No suelo aplicarlas	1	5%	3	12%	3	8%	1	3%	0	0%

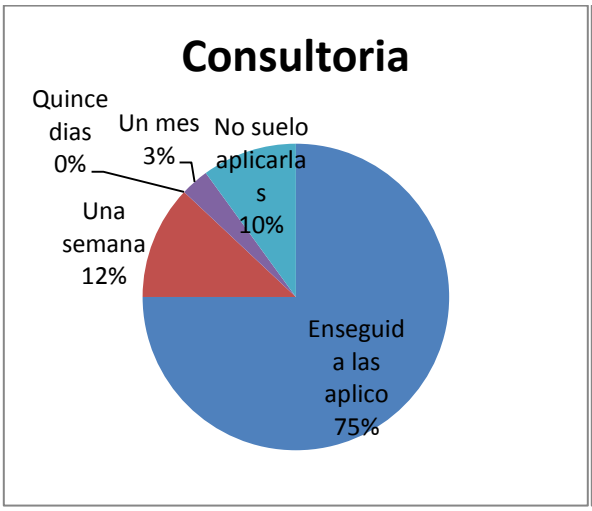


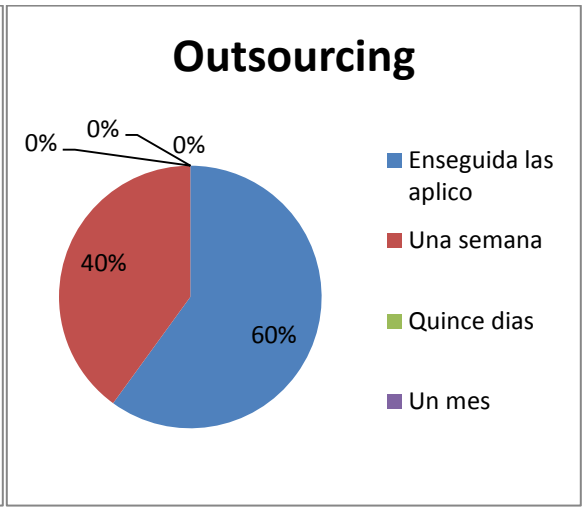
Comprobamos que si se analiza el tiempo que tardan en aplicar las nuevas medidas podemos ver que se respeta el mismo patrón mencionado en las respuestas anteriores ya que a medida que se crece en antigüedad aumenta es menor el tiempo que necesitan para aplicarlas. Un aspecto importante a destacar es que notamos una mayor dispersión en las respuestas entre las personas de 6 meses a 1 años.

Puesto	Asesoramiento		Auditoria		Consultoría		Outsourcing	
Enseguida las aplico	6	60%	45	75%	42	84%	3	60%
Una semana	1	10%	7	12%	4	8%	2	40%
Quince días	0	0%	0	0%	2	4%	0	0%
Un mes	2	20%	2	3%	1	2%	0	0%
No suelo aplicarlas	1	10%	6	10%	1	2%	0	0%









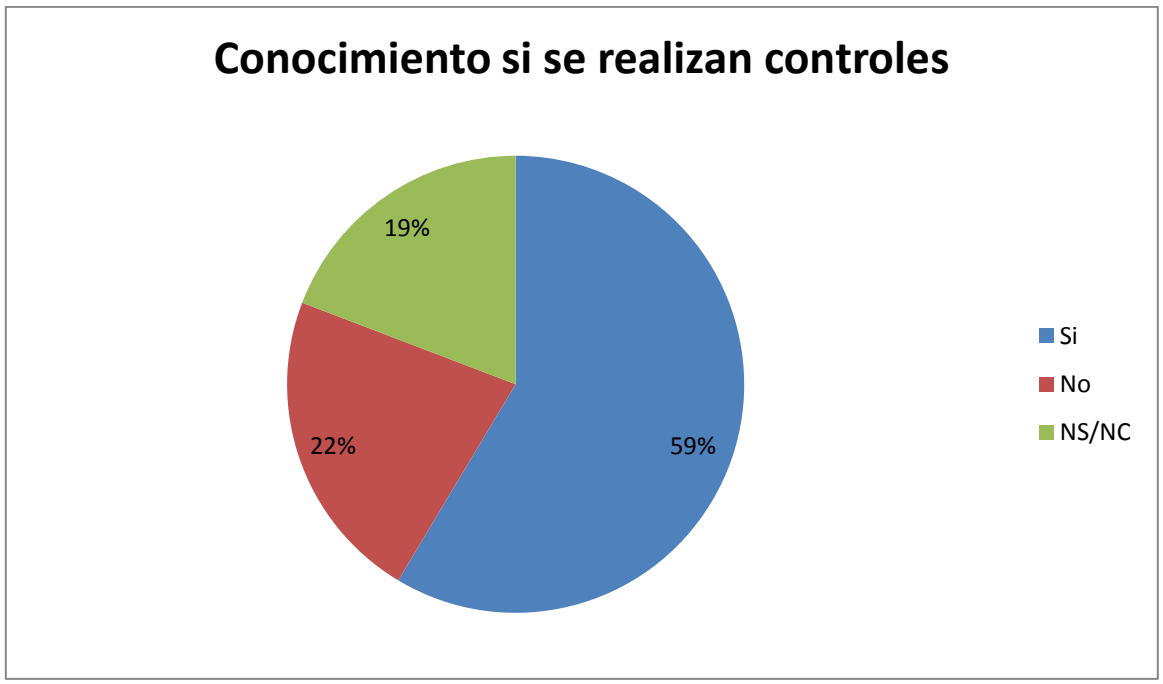
Si analizamos el tiempo que tardan en aplicarlos, consultoría es el área que tiene una adaptación más rápida y a quienes más les cuesta son las áreas de

asesoramiento y Outsourcing. Sin embargo el área de asesoramiento y auditoria tiene cada un 10% de los encuestados que dice que no suele aplicar las normas.

3.5.2.10 En la empresa donde trabaja o trabajó, indique si considera que se suelen realizar controles para evaluar el cumplimiento de las medidas de seguridad

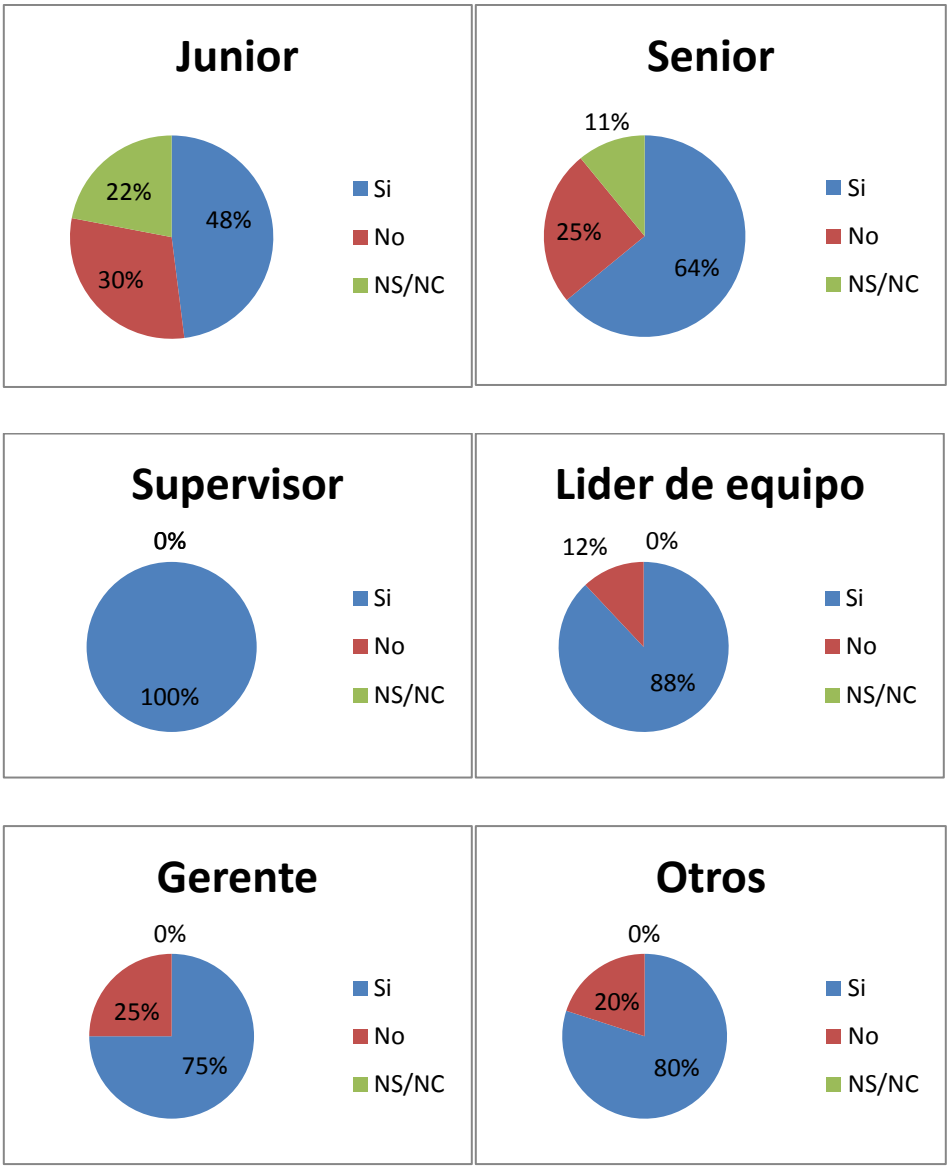
En este ítem buscamos evaluar el conocimiento que tienen los empleados acerca de que si se realizan controles en las empresas que trabajan.

	Empleados	%
Si	73	58%
No	28	22%
NS/NC	24	19%



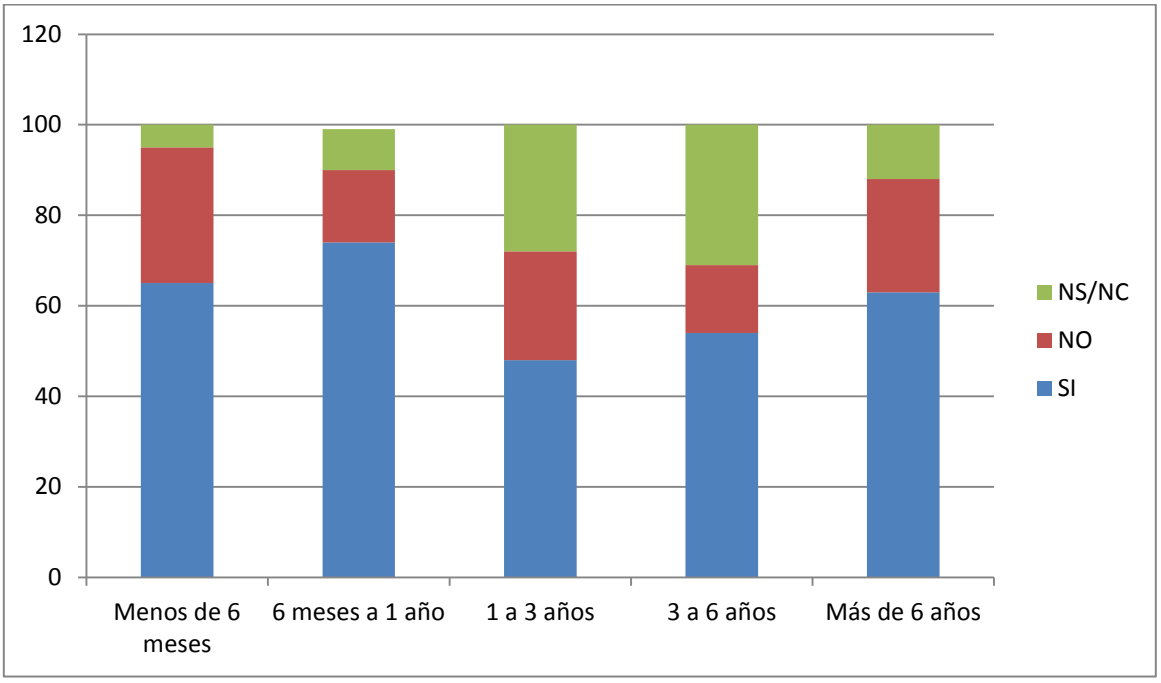
Se les consulto a los empleados si tenían conocimiento sobre controles que realiza la empresa sobre el cumplimiento de las normas y el 58% contesto que conoce que en su empresa se realicen controles, mientras que el 22% sabe que no se realizan. Hay un 19% de los encuestados que desconoce si en la empresa donde trabaja se realizan controles.

Puesto	Junior		Senior		Supervisor		Líder de equipo		Especialista		Gerente		Otros	
Si	33	48%	19	66%	6	100%	7	88%	1	25%	3	75%	4	80%
No	21	30%	3	10%	0	0%	1	12%	1	25%	1	25%	1	20%
NS/NC	15	22%	7	24%	0	0%	0	0%	2	50%	0	0%	0	0%



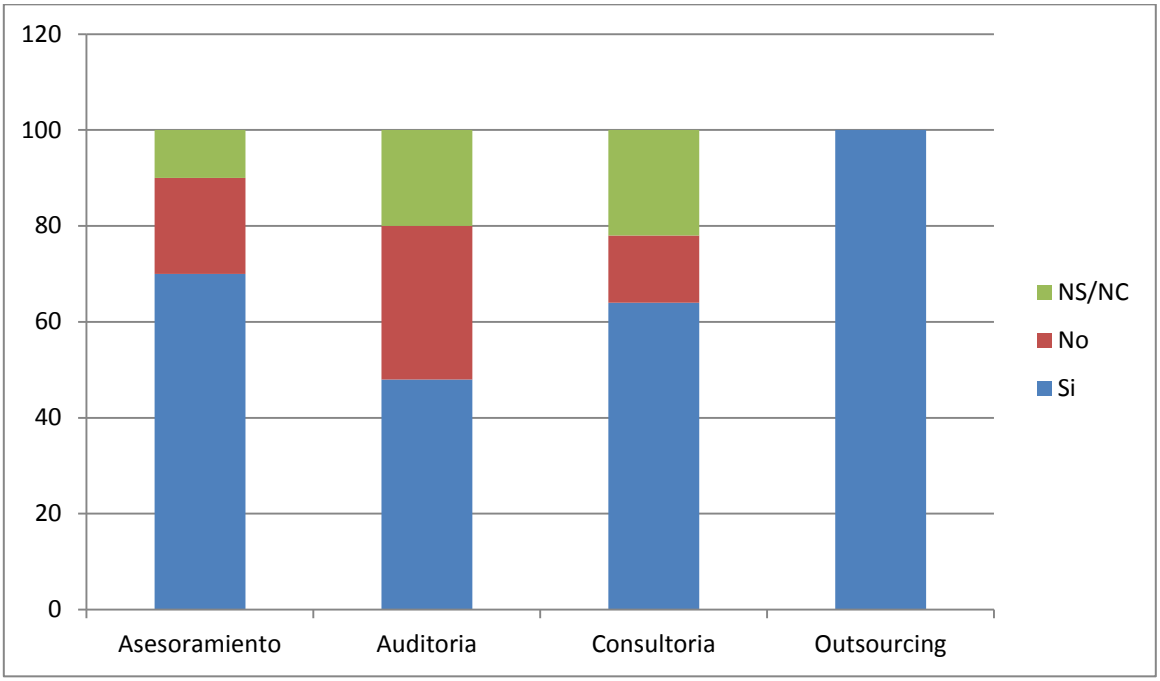
Podemos comprobar que a medida que ascienden en la escala jerárquica de la empresa el conocimiento hacia si se realizan controles va en aumento. Podemos notar que hay un débil conocimiento en los puestos juniors y seniors pero este se debe al poco tiempo que llevan en la empresa y el poco contacto que tienen con la auditoria de políticas.

Puesto	Menos de 6 meses		6 meses a 1 año		1 a 3 años		3 a 6 años		Más de 6 años	
Si	13	65%	17	74%	19	48%	14	54%	10	63%
No	6	30%	4	17%	10	24%	4	15%	4	25%
NS/NC	1	5%	2	9%	11	28%	8	31%	2	12%



Sorprendentemente podemos ver que en muchos casos los empleados con menor antigüedad si conocen que en su empresa se realizan controles. Podemos notar que en los empleados de 1 a 3 años y de 3 a 6 años hay un porcentaje de conocimiento mucho menor que en el que hay entre los empleados de menos de 6 meses o de 6 meses a 1 año.

Área	Asesoramiento		Auditoria		Consultoría		Outsourcing	
Si	7	70%	29	48%	32	64%	5	100%
No	2	20%	19	32%	7	14%	0	0%
NS/NC	1	10%	12	20%	11	22%	0	0%



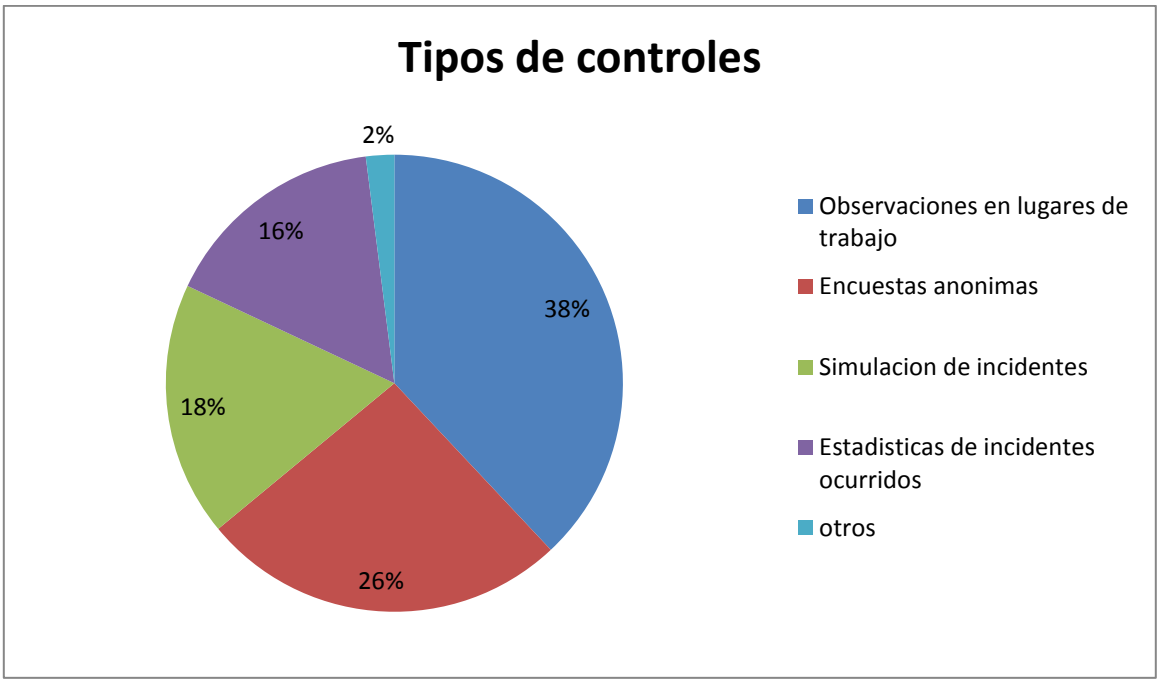
El área que más conoce si se hacen controles en su trabajo es el área de Outsourcing seguida por la de Asesoramiento. El área de auditoria es la que tiene un mayor porcentaje de empleados que dicen que no se realizan controles en las empresas donde trabajan.

En el área de consultoría se encuentran la mayor cantidad de empleados que desconocen si se hacen controles.

3.5.2.11 Tipos de controles que se realizan

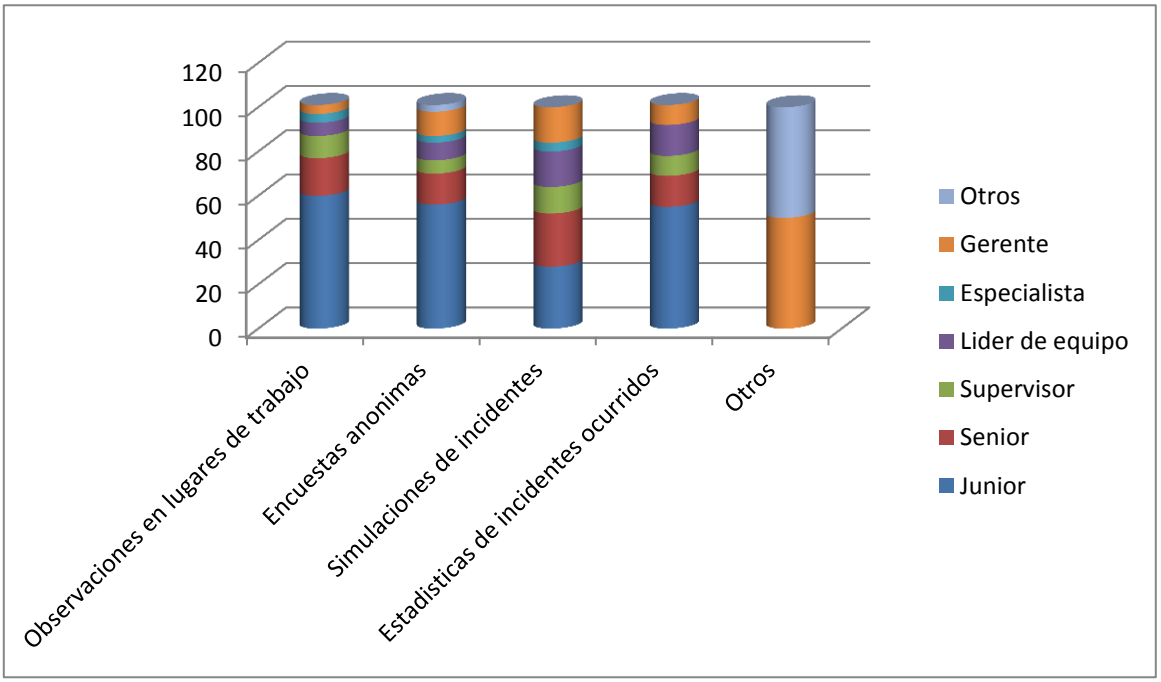
En este ítem se busca analizar si los empleados que dijeron que saben que en su empresa se realizan controles cuales son los mismos.

Controles	Empleados	%
Observaciones en lugares de trabajo	52	38%
Encuestas anónimas	36	26%
Simulaciones de incidentes	25	18%
Estadísticas de incidentes ocurridos	22	16%
Otros	2	1%



Entre los empleados que contestaron que si sabían que en sus empresas se realizaban controles el 38% contesto que estos se basan en observaciones en lugar de trabajo sorpresas, las encuestas anónimas se aplica en un 26% de los casos mientras que la simulación de incidentes y estadísticas de incidentes ocurridos tienen un 18% y 16% respectivamente.

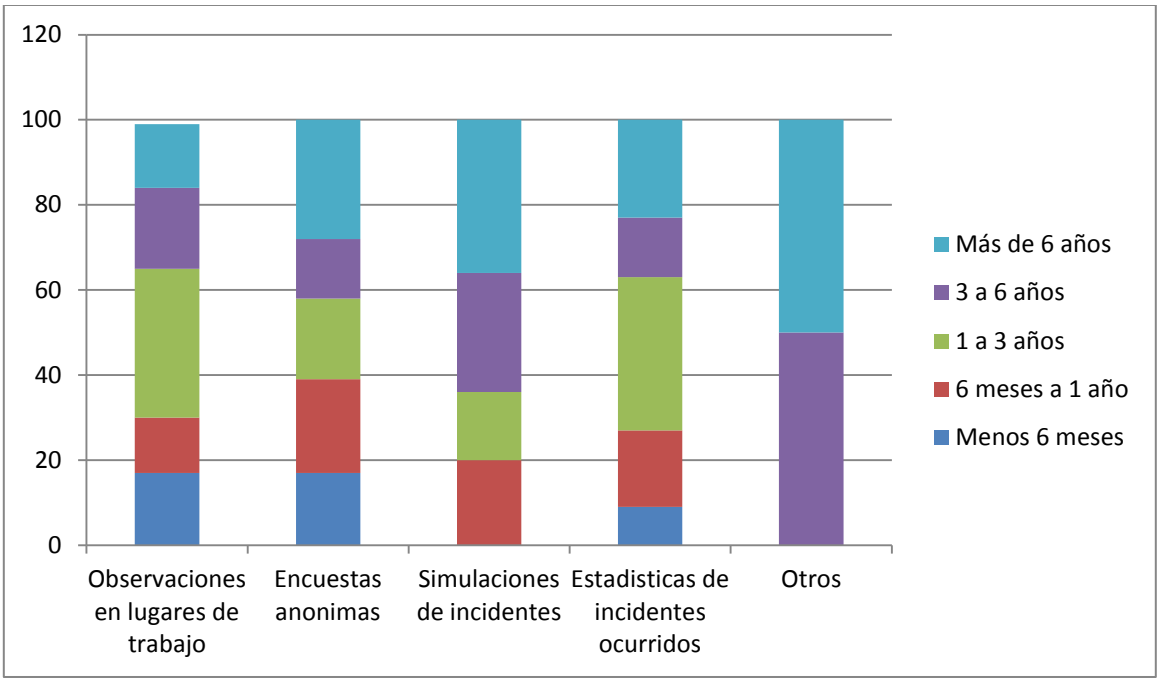
Puesto	Junior		Senior		Supervisor		Líder de equipo		Especialista		Gerente		Otros	
Observaciones en lugares de trabajo	31	60%	9	17%	5	10%	3	6%	2	4%	2	4%	0	0%
Encuestas anónimas	20	56%	5	14%	2	6%	3	8%	1	3%	4	11%	1	3%
Simulaciones de incidentes	7	28%	6	24%	3	12%	4	16%	1	4%	4	16%	0	0%
Estadísticas de incidentes ocurridos	12	55%	3	14%	2	9%	3	14%	0	0%	2	9%	0	0%
Otros	0	0%	0	0%	0	0%	0	0%	0	0%	1	50%	1	50%



.

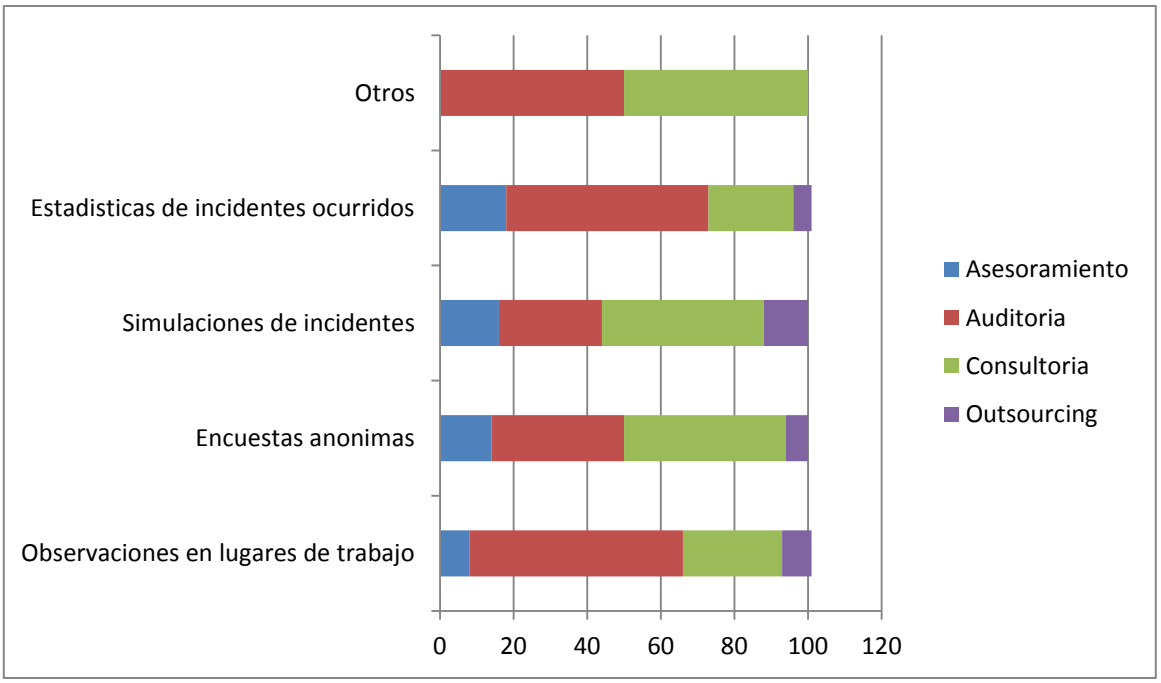
Si segmentamos por puesto podemos ver que el tipo de control varía mucho según el puesto que ocupan. Podemos ver que a los juniors son los que mayor control se le aplican ya que los mismos son los que más desconocimiento tienen de como operar.

Antigüedad	Menos 6 meses		6 meses a 1 año		1 a 3 años		3 a 6 años		Más de 6 años	
Observaciones en lugares de trabajo	9	17%	7	13%	18	35%	10	19%	8	15%
Encuestas anónimas	6	17%	8	22%	7	19%	5	14%	10	28%
Simulaciones de incidentes	0	0%	5	20%	4	16%	7	28%	9	36%
Estadísticas de incidentes ocurridos	2	9%	4	18%	8	36%	3	14%	5	23%
Otros	0	0%	0	0%	0	0%	1	50%	1	50%



En el caso de antigüedad podemos ver que las observaciones en lugares de trabajo aplican para los que llevan 1 a 3 años en la empresa mientras que las encuestas anónimas para los que trabajan hace más de 6 años al igual que la simulación de incidentes. Las estadísticas de incidentes ocurridos es mencionada también en mayor medida por los que llevan entre 1 a 3 años.

Área	Asesoramiento		Auditoria		Consultoría		Outsourcing	
Observaciones en lugares de trabajo	4	8%	30	58%	14	27%	4	8%
Encuestas anónimas	5	14%	13	36%	16	44%	2	6%
Simulaciones de incidentes	4	16%	7	28%	11	44%	3	12%
Estadísticas de incidentes ocurridos	4	18%	12	55%	5	23%	1	5%
Otros	0	0%	1	50%	1	50%	0	0%



Si analizamos las respuestas por áreas, las observaciones en lugares de trabajo corresponden a auditoria mientras que las encuestas anónimas a consultoría al igual que la simulación de incidentes. Las estadísticas de incidentes ocurridos es más conocida por los empleados de auditoria.

Aplicando la triangulación que utilizamos, encuestas a empleados de empresas de servicios profesionales (Big four), entrevistas a especialista de seguridad de la información y entrevistas a gerentes que lideran equipos que trabajan con información de terceros podemos concluir lo siguiente:

Según el especialista de IT de una Big Four las políticas de la casa matriz conforman la base para la implementación de la Norma ISO 2700. Desarrollando este proceso se generan las medidas operativas que realizan los empleados en sus actividades diarias para proteger la información que utilizan. Esto coincide en parte con las respuestas de los gerentes funcionales que dicen que las normas provienen de la casa matriz. Sin embargo, ambos concluyeron que desconocen si se basan en algún estándar internacional como si dijo la directora de operaciones de una big four.

Analizando las respuestas de los empleados podemos ver que el 72% de los encuestados entienden la importancia que tienen las medidas que la empresa les hace utilizar mientras que el 22% no las entiende lo cual, después hay un 6% que no sabe que responder frente a este tema. Esto es un aspecto a destacar ya que si los empleados no entienden bien que están haciendo es probable que haya errores en su aplicación y generen una probabilidad de fuga de la información.

En este aspecto podemos considerar que en estas empresas se crea una política desde la casa matriz para proteger la información ya que la mayoría de los empleados que trabajan en la mismas (90%) la consideran con una importancia alta y muy alta.

A pesar de que los empleados reconocieron que la información que manejan es sumamente elevada los empleados contestaron en un 90% que no consideran que una falta del cumplimiento en las normas de seguridad impuestas pueda generar una fuga de información. Pero es preocupante que sumado a cierto desconocimiento de parte de algunos empleados los gerentes de equipos consultados dijeron que desconocen que se debe hacer en caso de una fuga de información lo contrario a lo que dijeron los especialistas de que todo el personal de la empresa se encuentra preparado para el caso de una fuga de información.

Una de las formas de operacionalizar la norma ISO 27001 en las empresas es a través de los dominios que deben cumplir con determinadas características para lograr generar un entorno de seguridad. La aplicación de los dominios puede ir en el aspecto técnico, administrativo y físico. Dentro de las técnicas se encuentran controles de accesos, de los cuales el 96% de los encuestados dicen que lo aplican en sus empresas para acceder a la computadora y el 74% para los sitios web.

Analizando la información obtenida por los encuestados en el Ítem 7 obtenemos que las formas más comunes para acceder a la información son: vía mail según el 29% y el 28% acceden a un sitio en el cual se encuentra disponible por ello la mayoría de los gerentes funcionales mencionaron diversas medidas que se basan en proteger la información pero a su vez en un concepto de confianza integra en los empleados basándose en su ética y moral.

Si analizamos las respuestas obtenidas de los empleados las medidas más importantes después de las de validaciones de acceso se encuentran bloquear la computadora al alejarse del sitio de trabajo mencionada por los empleados en un 85% y el 81% destaco reiniciar las claves cada tres meses.

Los gerentes ya sean especialistas en el área o gerentes funcionales hablan de cómo cambian las medidas de seguridad que aplican los grupos de trabajo según el cliente con el que se trabaja. La realidad es que como las empresas de servicios profesionales aplican lo que se denomina las mejores prácticas en seguridad de la información no se deben realizar cambios fundamentales sino que los acuerdos de confidencialidad otorgan diferentes plazos y requisitos especiales que superan los estándares establecidos por las normas. En ninguno de los casos es posible disminuir los niveles de seguridad.

Un especialista en seguridad informática de una Big Four explica que los planes de capacitación se deben poder dividir entre los usuarios que van a llevar a cabo dichas medidas y los técnicos que regularizaran la actividad.

Según el mismo los planes de capacitación se basan en dar a conocer cuáles son los requisitos que el área de sistemas espera que se cumplan y a su vez una vez ya lograda la primera etapa se buscar refrescar periódicamente este conocimiento.

Analizando las respuestas obtenidas las dos formas más conocidas en las que se le dan a conocer a los empleados las nuevas políticas son e-mails y E-learning ambas con un 26% sobre el total de los encuestados.

Otro aspecto relevante a analizar es la practicidad que tienen estas medidas y la facilidad que tendrán los empleados para aplicarlas. Cuando se les consulto a los mismos cuanto tiempo les lleva adoptar como propias las nuevas medidas de seguridad el 77% contesto que lo hacía inmediatamente mientras que el 6% indico que nunca las aplicaba. Este es un aspecto preocupante ya que siendo el riesgo de fuga de información tan importante en este tipo de empresas que los empleados nunca apliquen las medidas de seguridad puede provocar daños irremediables.

Según un especialista de seguridad de informática de una empresa que se encarga de aplicar medidas de seguridad informática en otras empresas ara auditar los sistemas generales de seguridad de la información comento que se basan en la norma ISO 27005.

Sin embargo, el especialista de una Big Four explico que si bien se hacen controles no siempre estos son notados por el personal por eso se explica que solo el 58% de los encuestados haya contestado afirmativamente la pregunta de si en la empresa donde trabajaban se hacían controles.

Los controles mencionados por los encuestados fueron observaciones a lugares de trabajo por un 38% y encuestas anónimas por un 26%.

Para concluir, al consultarle a los gerentes funcionales y a los especialistas en seguridad informática como se procede en caso de un incidente. Los especialistas explicaron un plan en el cual se busca ver si se fallaron las políticas llevadas a cabo por la empresa o porque existe una nueva amenaza la cual la empresa no se había percatado. Sin embargo, los gerentes funcionales de equipo informaron que ellos

revisarían con sus equipos las formas de trabajo y se sentarían con sus superiores para buscar la forma de que lo mismo no vuelva a suceder.

Conclusión

A lo largo de nuestra investigación sobre la Seguridad de la Información en Empresas de Servicios Profesionales, en la cual se utilizaron para el trabajo de campo a las Empresas que conforman las Big Four en Argentina mencionadas en el Capítulo 2.1.2, hemos intentado responder los objetivos y preguntas establecidos al comienzo de nuestro trabajo:

- ¿Cuáles son las medidas llevadas a cabo por las empresas de servicios profesionales para la protección de la información de sus clientes?

Las medidas de seguridad que implementan las empresas de Servicios Profesionales se basan en la norma ISO 27001 (2.1.3) que toma como base a las políticas de Seguridad de la Información establecida por la Casa Matriz. Entre las medidas operativas más utilizadas, explicadas en el capítulo 2.2.2 y analizadas mediante el ítem 8 de las encuestas realizadas a los usuarios, y el ítem 2 de las entrevistas realizadas a los gerentes funcionales, encontramos como más importantes las siguientes: solicitud de contraseñas para acceder a la computadora, bloquear la computadora al alejarse de la misma, control de accesos tanto físicos como lógicos, monitoreo de la información en las computadoras, implementación de un sistema de antivirus, entre otras.

En general, mientras no se generen incidentes de seguridad que impliquen una fuga de información se considera que las medidas adoptadas fueron efectivas, debido a que las mismas cumplen con los estándares contenidos en la norma ISO 27001 mencionada en el párrafo anterior y se encuentran certificadas bajo su regulación. En el caso que surja algún incidente, está previsto realizar una investigación del mismo para analizar las causas y plantear cambios en los controles que impidan que este vuelva a suceder. Observamos también que los gerentes que conforman la línea media desconocen el plan de acción definido en caso de un incidente, debido a que no han enfrentado uno.

- ¿En qué grado se entienden y se cumplen estas medidas?

Podemos ver que hay un gran conocimiento de la importancia y características de la información con la que se trabaja (capítulo 2.2.1): confidencialidad, integridad y disponibilidad, y las mismas se tienen en cuenta al analizar los puntos críticos del negocio, que son importantes para determinar el nivel de seguridad que la empresa busca obtener (Ítem 8 – Entrevista Especialista IT). Las medidas adoptadas en la empresa son conocidas por los empleados y un 72% de ellos considera que las entiende, porcentaje que consideramos bajo teniendo en cuenta las características de la información que se intentan resguardar con las políticas implementadas. En este punto consideramos que hay una gran falencia de comunicación y conocimiento de los controles que se aplican para asegurar el cumplimiento de las mismas.

Con respecto al grado de aplicación y cumplimiento, hemos observado que el 88% de los encuestados según el ítem 14 de las encuestas considera que las normas son aplicadas por ellos en el plazo máximo de una semana, por lo cual afirmamos que el grado de cumplimiento es alto.

- ¿Es posible lograr un mayor grado de cumplimiento?

Con todo lo expuesto en los párrafos anteriores podemos concluir en base a la investigación realizada que las medidas de protección llevadas a cabo por las empresas de servicios profesionales en Argentina se cumplen y se conocen entre sus empleados, por lo tanto las mismas son efectivas. A pesar de eso, creemos que lograr una mejor comunicación con los empleados permitiría un mayor grado de información y entendimiento de las normas. El principal riesgo siempre es interno y proviene de los mismos empleados y aunque nunca se podrá reducir el riesgo en un 100%, siempre se podrán mejorar los resultados obtenidos con un principio de confianza en ellos.

Implicancias

Con respecto a la conclusión a la que llegamos en nuestra investigación, consideramos que debería lograrse que el empleado entienda la razón por la cual se aplican las medidas y no simplemente aplicarlas porque figuran como una obligación en las políticas de la empresa. Es por esto que surgen las siguientes implicancias como producto de nuestra investigación:

- Se sugiere poner un mayor énfasis en la creación de planes de capacitación para los empleados en general, en el cual se los instruya sobre los principales motivos por los cuales se aplican las medidas en lo que respecta a Seguridad de la Información. A su vez y teniendo en cuenta esta capacitación dada a los empleados, la gerencia debería permitir que los empleados puedan participar en la implementación y en la creación de nuevas medidas de seguridad
- Debido a la falencia de comunicación en especial del management con los mandos medios, se sugiere que para lograr un incluso mayor grado de cumplimiento de las medidas y políticas implementadas que el obtenido actualmente por la empresa se debería establecer un plan formal de comunicación especialmente dirigido a personas que ocupen cargos de Gerente o Gerente Senior, en el que se haga énfasis en los controles que se aplican y en los planes de acción ante un incidente presentes en la política de Seguridad de la Información de la empresa, para que los mismos sean conocidos y entendidos por los gerentes y sean capaces de llevarlos a cabo en caso de ser necesario y también como evitar que otro incidente de seguridad vuelva a ocurrir.
- Se sugiere crear otro plan de capacitación dirigido especialmente a cargos de Gerente o Gerente Senior, en el cual se los instruya con respecto a las medidas que se aplican, y a la razón por la cual se llevan a cabo acciones para proteger la información (Capítulos 2.2.1 y 2.2.3).

Bibliografía, Referencias y Recursos en Línea

Capítulo 1:

Actibva Magazine. Recuperado el 13 de Septiembre de 2014 de http://www.actibva.com/magazine/mercado-laboral/que-son-los-servicios-profesionales

Briano, J. C. et al. (2001).*Sistemas de información gerencial*. (1ª ed.) Buenos Aires: Prentice Hall.

Brigada de Investigación tecnológica. *Trabajo de Seguridad y protección de la información*. Recuperado el 8 de Noviembre de 2014 de http://spi1.nisu.org/recop/al02/bcorcoles/index.html

BSI Group. Recuperado el 20 de Septiembre de 2014 de http://www.bsigroup.es/es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001/

Chiavenato, I. (2006). *Introducción a la Teoría General de la Administración.* (7ª ed.) McGraw-Hill Interamericana.

Collazo, J. & Saroka, R. H. (2010). *Informática en las organizaciones* (1ª ed.). Buenos Aires: Consejo Profesional de Ciencias Económicas de la Ciudad de Buenos Aires.

Deloitte Argentina. Recuperado el 13 de Septiembre de 2014 de http://www.deloitte.com/view/es_AR/ar/servicios/index.htm

Economic, Contabilidad en línea. Recuperado el 13 de Septiembre de 2014 de http://www.e-conomic.es/programa/glosario/definicion-outsourcing

Ernst & Young Argentina. Recuperado el 13 de Septiembre de 2014 de http://www.ey.com/AR/es/Services

ISO 27000 en español. Recuperado el 20 de Septiembre de 2014 de http://www.iso27000.es/iso27000.html

ISO 27001 Standard. Recuperado el 20 de Septiembre de 2014 de http://www.iso27001standard.com/es/que-es-iso-27001/

KPMG Argentina. Recuperado el 13 de Septiembre de 2014 de http://www.kpmg.com/ar/es/servicios/Paginas/default.aspx

Lardent, Alberto. (2001). *Sistemas de información para la gestión empresaria*. (1ª ed.). Buenos Aires: Pearson Education.

Alvarado, L. *Administración de la Información.* Recuperado el 8 de Noviembre de 2014 de www.ucla.edu.ve%2Fdac%2FDepartamentos%2Fcoordinaciones%2Finformaticai%2Fdocumentos%2Fresumen%2520tema3.pdf&ei=C0pgVPPbH8yXNqeNgsgG&usg=AFQjCNGJN2YMsxuJICViJ7wpDLqlUvhKQw&sig2=rfZe-z6FxjawaEgN3Api-A&bvm=bv.79189006,d.cWc

Ministerio de Relaciones Exteriores y Culto de la República Argentina. Servicios Técnicos y Profesionales en Argentina.

Montuschi, L. (1999). La economía basada en el conocimiento.

Paños Álvarez, A. (1999). Reflexiones sobre el papel de la información como recurso competitivo de la empresa. *Canales de Documentación,* Nº2. 21-38.

Porter M. E. & Millar V. E. (1986). *Como obtener ventajas competitivas por medio de la información.* Harvard-Deusto Business Review.

Purificación Moscoso, Facultad de Documentación, Universidad de Alcalá (1998). Reflexiones en torno al concepto «Recurso de Información».

PWC Argentina. Recuperado el 13 de Septiembre de 2014 de http://www.pwc.com.ar/es/servicios/index.jhtml

Sans, M. C. (1998). Las normas ISO. *Biblio 3W. Revista Bibliográfica de Geografía y Ciencias Sociales*, Nº 129. Recuperado el 8 de Noviembre de 2014 de http://www.ub.edu/geocrit/b3w-129.htm

Stalk, G. (1988). *Time, the next source of competitive advantage.*Harvard Business Review.

Velasco Melo, A. H. (2008). El derecho informático y la gestión de la seguridad de la información.

Capítulo 2:

Álvarez Zurita, F. M. & García Guzmán P. A. (2007). Implementación de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001 para la Intranet de la Corporación Metropolitana de Salud.

Centro de Seguridad TIC de la Comunidad Valenciana. (nd.). 12 medidas básicas para la seguridad Informática. Recuperado el 8 de Noviembre de 2014 de http://www.csirtcv.gva.es%2Fsites%2Fall%2Ffiles%2Fdownloads%2F12%2520medidas%2520b%25C3%25A1sicas%2520para%2520la%2520seguridad%2520Inform%25C3%25A1tica.pdf&ei=9XxhVOP_A4qhgwSmr4F4&usg=AFQjCNFJhoyHPOmJBF3cAlKbDiY3dfTnQw&sig2=6yUoOaqDIjUKa7WD1KIE_A

Ciberataques: Los peligros que esconde la Red (2014).

Cols, C. (nd.). Políticas y Medidas de Seguridad. Recuperado el 10 de Noviembre de 2014 de http://.files.wordpress.com%2F2012%2F01%2Fpoliticas-y-medidas-de-seguridad.pptx&ei=MXphVIeTIYamNsj5guAO&usg=AFQjCNH4-8wcLy6AlbER6DJWMTm2DYRIoA&sig2=moEpDWHCl8Nu0OujenAgrg

Gualango Vega, R & Moscoso Montalvo P. (2011). Evaluación Técnica de la Seguridad Informática del Data Center de la Escuela Politécnica del Ejército. Recuperado el 8 de Noviembre de http://repositorio.espe.edu.ec%2Fhandle%2F21000%2F4279&ei=lG9hVIXuL8WYNuvDgaAE&usg=AFQjCNFi6-Aowy-uiuSnX4RHPEPtKqwYvQ&sig2=G8woF5nGMKDofmZVK_XtBQ

Huertas Calle, L. (2009). Políticas de seguridad informática, tácticas para hacerlas efectivas. Recuperado el 8 de Noviembre de 2014 de http://www.slideshare.net/SamuraiBlanco/politicas-seguridad-leonardo-huertas

Joyanes, L. (2009). Cloud Computing: El nuevo paradigma tecnológico para empresas y organizaciones en la Sociedad del Conocimiento. Recuperado el 22 de Septiembre de 2014 de http://gissicmexico.wordpress.com/2009/03/03/cloud-computing/

Reed, S. (2008). Riesgos y amenazas de la fuga de información en las empresas. *Perspectiva Empresarial*, Nº20.

RIO ALTO MINING LIMITED. POLITICA DE DIVULGACIÓN DE INFORMACIÓN Y CONFIDENCIALIDAD (2012).

Universidad Nacional de Colombia. (2003). Guía para elaboración de políticas de Seguridad. Recuperado el 8 de Noviembre de 2014 de http://.dnic.unal.edu.co%2Fdocs%2Fguia_para_elaborar_politicas_v1_0.pdf&ei=4HphVKjSHMWlNsemgYgO&usg=AFQjCNH-qW6_AZd9gkSZODrK-rZux15ldQ&sig2=44bC09H_by64gxK8-JqDTA

Voutssas M. J. (2010). Preservación documental digital y seguridad informática. Investigación bibliotecológica, 24(50), 127-155. Recuperado en 22 de octubre de 2014, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008&lng=es&tlng=es.

Capítulo 3:

Aguilera López, P. (2010). *Seguridad Informática*. Editex.

Alonso, P. (nd.). Delitos contra la Confidencialidad, Integridad y Disponibilidad de los Datos y Sistemas Informáticos.

Hernández Hernández, E. (1995).*Auditoria en Informática*. 1ª ed. México: Compañía Editorial Continental.

ISO Tool Excellence. Recuperado el 10 de Noviembre de 2014 de http://www.isotools.cl/isoiec-27007/

Joyanes, L. & Vaquero, A. (1993). *Informática: Glosario de Términos y Siglas*. (1a ed.). España, Madrid: McGraw-Hill.

Moreno Bravo, J. (2012). Auditoria Informática. Recuperado el 10 de Noviembre de 2014 de http://www.slideshare.net/j_moreno/auditoria-informatica-y-de-sistemas-de-informacion

Robles, R. & Rodríguez de Roa, A. (2006). La gestión de la seguridad en la empresa.

Royer, J. M. (2004). *Seguridad en la Informática de Empresa: Riesgos, Amenazas, Prevención y Soluciones*. Paris: ENI.

Marco metodológico:

Blázquez Entonado, F. (1988). Evaluación Del Rendimiento en la Enseñanza Superior. Madrid: Centro de Investigación y Documentación Educativa.

Grinnell (1997) citado por Hernández, R.; Fernández, C. y Baptista, P. (2006) Metodología de la Investigación. México: Editorial Mc Graw Hill.

Kuhn, T. S. (1962). *La estructura de las Revoluciones Científicas*. The University of Chicago Press.

Kuhn, T. S. (1970). *La estructura de las Revoluciones Científicas*. The University of Chicago Press.

Malhotra, N. K. (2010). *Investigación de Mercados*. (5ª ed.). México: Pearson Education.

Anexo

Entrevista a la Directora de Operaciones de una Big Four

1) ¿Cuáles son las acciones que lleva a cabo un equipo de trabajo de empresas de servicios profesionales para proteger la información? ¿Considera que cumplen algún estándar internacional?

La firma sigue la política global de la casa matriz, que está basada en la ISO 27001.

2) ¿Cuáles son los controles más comunes que se llevan a cabo para asegurar el cumplimiento de las medidas aplicadas respecto de la seguridad de la información?

Control físico de accesos (tarjeta de acceso personal por empleado). Control de Acceso al sistema con usuario y password personal con bloqueo luego de una cantidad determina de intentos fallidos. Control de anti-virus (se generan reportes). Controles de software, etc. Encripción de la información para proteger dispositivos móviles (discos rígidos, pen drives, teléfonos).

3) Cuando se empieza a trabajar con algún nuevo cliente, ¿Deben que deben adaptarse y modificarse algunas prácticas habituales? ¿Esto presentaría alguna dificultad en un grupo de trabajo?

En general ante un cliente nuevo no deben modificarse las prácticas habituales. En cualquier caso nunca podría implicar reducir el nivel de seguridad de la información.

4) ¿Cómo se comunican a los grupos de trabajo las mejores prácticas a llevarse a cabo con respecto a la seguridad de la información? ¿Cómo se capacita al empleado sobre este tema?

Se comunica a través un portal de intranet, en el cuál se publican las políticas y procedimientos relacionados con seguridad de la información, tendientes a reforzar las medidas de seguridad existentes, por ejemplo uso de pendrives encriptados, etc.

Curso de seguridad de la información: Es requerido como curso previo a que el empleado comience a trabajar con información de clientes. Cursos de refuerzos a cargo de personal de Seguridad de la información.

5) ¿Podría describir las características más importantes de la información con la que trabaja?

Confidencialidad, disponibilidad, integridad

6) En el trascurso de la actividad diaria, ¿Es fácil identificar los riesgos que pueden surgir del mal uso de la información?

La identificación de los riesgos es simple. Lo más complejo es mitigarlos. Hay un principio básico de confianza en el empleado. Probabilidad de ocurrencia y el impacto.

7) En el caso de una fuga de información, ¿Existe algún plan de acción definido? ¿En qué consiste?

Hay un plan de manejo de incidentes de seguridad que incluye un plan de escalamiento y comunicación, colección de evidencia y posterior remediación, con roles y responsabilidades definidas. Fases definidas: 1) preparación 2) detección y análisis, 3) contención erradicación y recupero, 4) Actividad post incidente.

Existe un Comité de Information Security y Data Protection cuyo objetivo es revisar, proponer y aprobar las políticas de seguridad de la información y protección de datos. Este comité periódicamente revisa el estado general de seguridad de la información, notifica al Comité de accionistas y directorio sobre los issues identificados en auditorías internas y externas. Asimismo, analiza los casos que podrían ser incidentes de seguridad de la información y toma decisiones al respecto. Por último promueve la concientización de la seguridad de la información en toda la organización.

8) ¿Cuáles son las acciones correctivas que se llevan a cabo para que el mismo no vuelva a ocurrir?

Depende del incidente que se haya generado, se revisarán los controles para evitar que esa fuga de información vuelva a ocurrir.

Entrevista a un Gerente Funcional de una Big Four (1)

1) ¿Cuáles son las acciones que lleva a cabo un equipo de trabajo de empresas de servicios profesionales para proteger la información? ¿Considera que cumplen algún estándar internacional?

Las acciones más comunes son: encriptación de archivos, usuarios sin perfil de acceso a modificación de datos, cable de seguridad en las notebooks, charlas periódicas de los encargados de seguridad informática, puertas de acceso a oficinas con seguridad, claves de acceso. Las políticas de seguridad son requeridas por Casa Matriz.

2) ¿Cuáles son los controles más comunes que se llevan a cabo para asegurar el cumplimiento de las medidas aplicadas respecto de la seguridad de la información?

Bloqueo a determinadas páginas que pueden presentar algún riesgo, modificación de claves de acceso en forma periódica, monitoreo de la información (encriptación de archivos que se envían por email, por pen drive).

3) Cuando se empieza a trabajar con algún nuevo cliente, ¿Deben que deben adaptarse y modificarse algunas prácticas habituales? ¿Esto presentaría alguna dificultad en un grupo de trabajo?

En algunas oportunidades, por la característica del cliente, necesitamos acceso a determinada información, y debemos solicitar permisos para acceder a la misma.

4) ¿Cómo se comunican a los grupos de trabajo las mejores prácticas a llevarse a cabo con respecto a la seguridad de la información? ¿Cómo se capacita al empleado sobre este tema?

Charlas periódicas para reforzar.

5) ¿Podría describir las características más importantes de la información con la que trabaja?

Información restringida de clientes, inciden en toma de decisiones.

6) En el trascurso de la actividad diaria, ¿Es fácil identificar los riesgos que pueden surgir del mal uso de la información?

Si, la información que se maneja influye en toma de decisiones.

7) En el caso de una fuga de información, ¿Existe algún plan de acción definido? ¿En qué consiste?

No he tenido conocimiento de fuga de información.

8) ¿Cuáles son las acciones correctivas que se llevan a cabo para que el mismo no vuelva a ocurrir?

N/A

Entrevista a un Gerente Funcional de una Big Four (2)

1) ¿Cuáles son las acciones que lleva a cabo un equipo de trabajo de empresas de servicios profesionales para proteger la información? ¿Considera que cumplen algún estándar internacional?

Particularmente en la firma en la que trabajo contamos con un área que se especializa en la seguridad de la información, definiendo constantemente políticas y medidas a seguir todos los miembros de la firma para proteger tanto la información de nuestros clientes como la propia.

Las acciones que tomamos en mi equipo de trabajo principalmente son: asegurarnos de no incluir en nuestros mails información confidencial o delicada, y utilizar las herramientas previstas por la firma para el intercambio de información con el cliente. La herramienta más importante que utilizamos en un repositorio on-line el cual es administrado por determinadas personas de la firma las cuales definen los accesos de cada persona (de mi equipo y del cliente), como así también las acciones que puede realizar en el mismo (restricciones de visualización, descarga de archivos, permisos de modificación, etc.).

En cuanto al envío de información confidencial vía mail, no existe nada que pueda evitar que una persona envíe algo que no debe. Esto está en la conciencia y en la moral de cada persona, y en los líderes de los equipos para concientizar a la gente.

En cuanto a si cumplimos con algún estándar internacional lo desconozco, pero creería que si porque la firma es internacional y porque el volumen de información que administra de los clientes es muy grande.

2) ¿Cuáles son los controles más comunes que se llevan a cabo para asegurar el cumplimiento de las medidas aplicadas respecto de la seguridad de la información?

En mi equipo de trabajo no realizamos controles específicos más que controlar la información que incluimos en los mails. Siempre seguimos las indicaciones y recomendaciones que recibimos de nuestro equipo de Seguridad informática, entendiendo que al cumplir con esto estamos protegiendo la información.

3) Cuando se empieza a trabajar con algún nuevo cliente, ¿Deben que deben adaptarse y modificarse algunas prácticas habituales? ¿Esto presentaría alguna dificultad en un grupo de trabajo?

Dependiendo de la envergadura del cliente y la exposición pública nos vemos obligados a incluir nuevas medidas, las cuales en la mayoría de los casos lo solicita el cliente.

He trabajado en muchas empresas de Sector Público y algunas de ellas nos han solicitado que todos los miembros de nuestro equipo firmen un documento en el cual se comprometen a no divulgar información alguna con ninguna otra persona que no sea del proyecto, ni siquiera familiares. Recuerdo que en un proyecto esto nos trajo problemas con nuestro equipo porque además de que la nota decía que no se podía divulgar información además existían penalidades que caían sobre cada miembro del equipo, y obviamente nadie quería firmarlo.

4) ¿Cómo se comunican a los grupos de trabajo las mejores prácticas a llevarse a cabo con respecto a la seguridad de la información? ¿Cómo se capacita al empleado sobre este tema?

Las comunicaciones que recibimos del área de Seguridad Informática son siempre vía mail y constantes. Las comunicaciones van desde recordatorios para modificar regularmente las passwords hasta requerir llevar nuestras máquinas para que procedan a instalar aplicaciones que protegen la información que tenemos.

No es común que se dicten capacitaciones presenciales, todo se realiza vía mail o en algunas oportunidades debemos realizar un curso on line.

5) ¿Podría describir las características más importantes de la información con la que trabaja?

Principalmente trabajamos con información crítica y muy confidencial porque trabajamos en el área Financiera, con muchos números e indicadores como ser, volúmenes de ventas, volúmenes de pagos, inversiones, contrataciones, rentabilidad, etc. Se trata de información muy sensible ya que evidencia cuál es la estrategia de negocio que tiene la compañía.

6) En el trascurso de la actividad diaria, ¿Es fácil identificar los riesgos que pueden surgir del mal uso de la información?

En nuestro negocio los riesgos son casi siempre los mismos, obviamente que dependiendo de la envergadura del cliente los riesgos tienen distinto grado de

impacto. Cuando se trata de proyectos en lo que participan muchas personas la identificación de los riesgos, pero por sobre todo el control, no es tan fácil de llevar a cabo. En mi caso me apoyo mucho en las herramientas que utilizamos para la gestión de nuestro trabajo para minimizar los riesgos.

7) En el caso de una fuga de información, ¿Existe algún plan de acción definido? ¿En qué consiste?

Desconozco si existe algún plan de acción, pero mi forma de actuar sería en primer lugar elevar el caso a mi superior inmediato y a continuación se lo comunicaría a nuestro equipo de Seguridad Informática para que me asesore en las acciones a seguir.

8) ¿Cuáles son las acciones correctivas que se llevan a cabo para que el mismo no vuelva a ocurrir?

Eso dependerá de cuál haya sido el problema, si se trata de un problema relacionado a la falta de control en algunas de las herramientas que utilizamos entiendo que se deberían mejorar los sistemas (solución técnica), y si se trata de otro tipo de error se revisarían los procedimientos a fin de ajustarlos y evitar que vuelva a dar el caso (solución en procedimiento).

Entrevista a un Gerente de IT especialista en Seguridad de la Información de una Big Four

1) Con respecto a la Norma ISO 27001, ¿Cómo es la implementación en una empresa de servicios profesionales?

Se parte de una política que está basada en la norma, esta política vendría a ser la “ley” y es bastante compleja, pero es distinta de la que le llega al usuario final, es decir, a los empleados, a ellos les llega un “Manual de seguridad” que se desprende de esta política.

Para proceder a la implementación de la norma hay que partir de una política.

2) ¿Cómo se aplican los dominios que forman parte de la Norma?

Los dominios de la norma se aplican mediante un conjunto de controles, algunos de ellos son más técnicos y otros de ellos son más administrativos, incluso algunos de estos controles no se pueden demostrar.

Cada uno de estos controles indican los requisitos que cada dominio debe cumplir para crear un entorno seguro.

3) ¿Podría comentarnos acerca de las mejores prácticas con respecto a la Seguridad de la Información?

Las mejores prácticas se llevan a cabo mediante normas, ya que hay empresas que se encargan de certificarlas. Para el caso de empresas europeas, se suele certificar ISO 27001, y para empresas americanas se certifican las normas SOC (SOC 3, SOC2). Es decir que las mejores prácticas están contenidas en estas normas.

4) ¿Deben realizarse cambios en el sistema de trabajo cuando se empieza a trabajar con un nuevo cliente?

Por lo general no es necesario hacer cambios ni en las medidas adoptadas ni en el sistema de trabajo al operar con un nuevo cliente, a menos que este tenga requerimientos especiales.

Es importante destacar que, de ser necesario realizar algún cambio, solo va a ser posible hacerlo mientras no atente con la política actual de la empresa.

5) ¿Cuáles son las complejidades que se deben enfrentar en la implementación de un SGSI?

La principal complejidad que se debe enfrentar es tratar de encontrar un equilibrio entre la seguridad y la practicidad para llevar a cabo el negocio, es decir crear un entorno de seguridad aceptable dentro de un negocio rentable, esto representa un desafío ya que implica lograr un equilibrio entre costo y beneficio. Por ejemplo no tiene sentido invertir en un sistema de encriptación de archivos si no contamos con

discos móviles. Hay que ver el impacto de una posible amenaza en la brecha de seguridad y hasta qué punto conviene invertir, tengo que ver que es lo más crítico para mi negocio para mi negocio teniendo en cuenta las 3 características de la información: confidencialidad, integridad y disponibilidad.

6) ¿Cuáles son los puntos en los que se enfoca una capacitación en este tema con periodicidad?

Primero y principal las capacitaciones deberían estar orientadas a la persona que va a trabajar, que no sería la misma capacitación que tendría alguien con una orientación más técnica, por esto es importante establecer el público objetivo, no tiene que ser la misma capacitación para todos.

Las comunicaciones deberían ser periódicas para que sean efectivas y se pueden dar en muchos medios: e-learnings, mails, cursos y charlas presenciales.

7) ¿Cuáles son las medidas técnicas que se llevan a cabo en la implementación de un SGSI?

Las medidas técnicas más importantes, es decir críticas son:

- Instalación e implementación de un sistema de antivirus
- Securizacion perimetral de la red (creación de un firewall, IPS, IDS)
- Manejo de vulnerabilidades y patching

8) ¿En que se basa el análisis de riesgos en materia de seguridad de la información?

En el análisis de los riesgos se tiene que tener en cuenta la combinación de dos factores: la probabilidad de ocurrencia del riesgo (que puede ser mitigada mediante un UPS por ejemplo) y el impacto en el negocio que podría implicar este riesgo de materializarse. La lógica seria la siguiente: a medida que suben la probabilidad de

ocurrencia y el impacto en el negocio, aumenta el riesgo. El mayor riesgo siempre viene del lado del usuario interno, es decir el empleado mismo.

Entonces el risk assesment consiste en mitigar o aceptar el riesgo, si el mismo no es crítico para el negocio, como siempre hay que buscar el equilibrio entre el costo y el beneficio, ya que una mayor seguridad conlleva mayores costos.

9) Luego de un incidente, ¿Qué aspectos se analizan para evitar que vuelva a suceder?

En primer lugar se aísla el incidente para que el mismo no se propague. Esto implica una actividad “forensic”, analizar el incidente para ver cuál fue la causa original y cuáles fueron las fallas, para que no vuelva a suceder. Esto se suele hacer por ejemplo mediante la implementación de nuevos controles.

10) ¿Cómo se caracteriza el proceso de auditoría de un SGSI?

En una auditoria se analizan los controles, aunque algunos de ellos no son comprobables, y también pueden llegar a pedirse evidencias.

Entrevista a un especialista en Seguridad de la Información certificado en ISO

1) Con respecto a la Norma ISO 27001, ¿Cómo es la implementación en una empresa de servicios profesionales?

De manera general, se siguen una serie de actividades que son aplicables a cualquier tipo de organización, puesto que el estándar es de aplicación general, sin importar si se trata de una empresa grande o pequeña, pública o privada.

Previo a la implementación del estándar, es necesario que se cumplan algunas condiciones, principalmente que se tenga el patrocinio de la alta dirección para llevar a cabo todas las iniciativas relacionadas con el sistema de gestión, así como contar con los recursos necesarios para su planeación, implementación, revisión y mejora.

Luego de lo anterior, la primera actividad para el SGSI consiste en entender las necesidades y expectativas de las partes interesadas, así como definir el alcance del SGSI. Esto resulta importante debido a que todo lo relacionado con el sistema debe estar limitado por estas necesidades y el alcance, que puede ser desde un proceso de negocio, unidad dentro de la organización, área funcional o cualquiera que la organización determine.

También es necesario contar con una política de seguridad de la información, una evaluación de riesgos, la declaración de aplicabilidad, el plan de tratamiento de riesgos, auditorías y revisiones por parte de la dirección con relación al SGSI, así como evidencia de acciones correctivas, entre otras actividades.

Para evitar enlistar todas las actividades, basta con mencionar que se deben cumplir de manera obligatoria las cláusulas 4 a la 10 de la versión de 2013 del estándar, en caso de que la organización busque obtener la certificación. Si se trabaja con la versión del 2005, es necesario cumplir con las cláusulas 4 a la 8.

Los controles de seguridad considerados en el Anexo A pueden ser seleccionados con base en los resultados de una evaluación de riesgos. Los controles descartados con base en estos resultados, necesitan una justificación para su exclusión.

2) ¿Cómo se aplican los dominios que forman parte de la Norma?

La aplicación de los controles de seguridad considerados en los dominios del Anexo A, son el resultado de una evaluación de riesgos, es decir, de la identificación, análisis y valoración de todas aquellas amenazas que podrían materializarse y afectar de manera negativa los activos más importantes de una organización (incluida la información), y por lo tanto, impactar en los objetivos y misión de la misma.

Con base en esta evaluación, que puede ser de carácter cualitativa o cuantitativa, se genera un documento denominado Declaración de Aplicabilidad (SoA por sus siglas en inglés), donde se plasman los controles de los dominios que han sido seleccionados para mitigar los riesgos evaluados (los controles pueden ser técnicos, físicos o administrativos). Posteriormente, se debe generar y ejecutar un plan de

tratamiento de riesgos, en donde se define la forma en la cual serán aplicados estos controles de seguridad seleccionados.

3) ¿Podría comentarnos acerca de las mejores prácticas con respecto a la Seguridad de la Información?

Las mejores prácticas son un conjunto de acciones, metodologías, herramientas y técnicas que han sido aplicadas y probadas en un contexto determinado, y que han producido resultados considerados como buenos respecto a los objetivos establecidos.

Algunas de estas mejores prácticas son consideradas para formar parte de algún estándar, como es el caso de los estándares ISO, cuya principal diferencia radica en el hecho de que son certificables para las organizaciones.

En el ámbito de la seguridad de la información, existen diferentes marcos o frameworks que agrupan y promueven estas prácticas, algunos certificables y otros no. En cuestión de estándares, una referencia internacionalmente utilizada es ISO 27001, pero existen otros enfocados en seguridad de la información como es el caso de los estándares NIST.

Otros frameworks como COBIT, cuentan con publicaciones específicas para seguridad de la información (COBIT for Information Security) y otras mejores prácticas contribuyen a una mejor implementación de los controles de seguridad, por ejemplo, la gestión de servicios considerada en ITIL.

4) ¿Deben realizarse cambios en el sistema de trabajo cuando se empieza a trabajar con un nuevo cliente?

Los cambios están en función de las medidas de seguridad que han sido consideradas para proteger la información de la organización o de los clientes. Estas medidas son el resultado de la selección de los controles en la declaración de aplicabilidad.

En ocasiones, los clientes son quienes definen requisitos y controles de seguridad para el manejo de su información, por lo que será necesario llevar a cabo modificaciones relacionadas con la operación de la organización, con base en esas necesidades y características.

5) ¿Cuáles son las complejidades que se deben enfrentar en la implementación de un SGSI?

Existen diferentes dificultades que pueden presentarse cuando se inicia la implementación del sistema de gestión, que pueden ir desde cuestiones administrativas, técnicas, legales, incluso de cultura laboral.

Por ejemplo, la resistencia al cambio puede ser un factor a considerar, ya que el personal puede oponer cierta resistencia si sus actividades se ven modificadas de acuerdo a las que realizaba de manera periódica.

6) ¿Cuáles son las medidas técnicas que se llevan a cabo en la implementación de un SGSI?

Como ya se mencionó, los controles de seguridad del tipo técnico dependerán del resultado de la evaluación de riesgos. En general, la referencia para estas medidas es el Anexo A del estándar, sin embargo no están limitadas a esta propuesta, ya que pueden incluirse otro controles de diferentes marcos de trabajo.

Por ejemplo, algunos medidas consideran controles contra malware, controles de red y servicios de red, medidas de seguridad durante el desarrollo de software, etc.

7) ¿Existe algún método de análisis de riesgos en materia de seguridad de la información?

En realidad existen varios métodos o metodologías para la evaluación de riesgos, mismas que pueden o deberían alinearse a un proceso de gestión de riesgos. La evaluación de riesgos solamente es una fase del proceso de gestión de riesgos.

El estándar ISO 27005 describe un proceso para gestionar riesgos, mismo que debe ser complementado con algún método o metodología que permita evaluar los riesgos de seguridad asociados a los activos de la organización.

Por mencionar algunas, existen opciones como OCTAVE Allegro, NIST 800-30, CORBA, FRAP, entre otras. Algunos son accesibles de forma gratuita y otras requieren que se realice un pago para poder utilizar el método.

8) Luego de un incidente, ¿Se llevan a cabo acciones correctivas para que el mismo no vuelva a ocurrir?

De preferencia se llevan a cabo acciones que permitan corregir alguna condición que haya derivado de un incidente. Sin embargo, es importante mencionar que las acciones correctivas no solo se aplican como consecuencia de un incidente, si no que pueden ser resultado de otros factores, como auditorías internas, sugerencias, acciones de mejora, revisiones de la alta dirección. El objetivo de las acciones correctivas es dar una solución y erradicar los problemas desde su origen para que no puedan materializarse nuevamente.

El proceso de gestión de incidentes utiliza un enfoque de seguridad reactivo y se trata de un control incluido en el Anexo A que puede operar de manera paralela a otros procesos, como el de gestión de riesgos o de medición del SGSI.

9) ¿Cómo se caracteriza el proceso de auditoría de un SGSI?

El proceso de auditoría sigue los lineamientos descritos en el estándar ISO 19011 o también se puede utilizar como referencia ISO 27007, que tiene como base ISO 19011.

De manera general, es necesario crear un programa de auditorías para el SGSI, que incluya la frecuencia de las auditorías, métodos, responsabilidades, planeación, así como la forma de entrega de los informes de resultados de dichas auditorías.

También, debe considerar los criterios y alcance de la o las auditorías, así como la selección de los auditores, que garantice la objetividad e imparcialidad en los resultados.