El Conocimiento Organizacional

Descubriendo Decisiones

Autores:
Dr. Sergio Daniel Conde
Ing. Osvaldo Marcovecchio

Tercera Edición

La seguridad de la información.

Introducción

Hace relativamente pocos años la seguridad de la información era de fácil administración, sólo bastaba con guardar los documentos más importantes bajo llave y brindar protección a los empleados que poseían el conocimiento. Hoy en día esto es mucho más difícil. Con la evolución de los sistemas electrónicos, que han permitido automatizar un sin número de procesos y brindar grandes ventajas por su capacidad de almacenamiento y procesamiento, se han ido constituyendo como un componente fundamental en todas las organizaciones, pero al mismo tiempo se debería desarrollar sistemas que permitan preservar la seguridad de los activos de información y evolucionar conjuntamente para mantenerse al día con la tecnología cambiante. Con la llegada de Internet han surgido los crímenes cibernéticos que causan grandes gastos y pérdidas muy significativas por no mantener seguridad de la información.

El objetivo fundamental de la seguridad de la información es reducir los riesgos y dar soporte a las operaciones del negocio, pues implementar una solución cien por ciento segura no existe, sólo es posible realizar un proceso de mitigación de riesgos.

Seguridad de la información vs. Seguridad informática

Antes que nada, debemos dejar en claro a qué nos referimos cuando hablamos de seguridad de la información, y a qué cuando hablamos de seguridad informática. Hoy en día, es muy común escuchar en diferentes ámbitos estos dos términos como si tuvieran la misma definición, cosa que no es así. Y es fundamental conocer bien la diferencia.

La seguridad informática es el área encargada de la protección de las infraestructuras de las Tecnologías de la Información y Comunicación, en adelante TIC. Por ejemplo: en seguridad informática, podemos implementar algunos controles para la protección del equipamiento informático y de los sistemas de información contra ataques o códigos maliciosos, como AntiVirus y CortaFuegos (Firewall).

En cambio, la seguridad de la información es el área encargada de la protección de los activos de información en cuanto a las siguientes propiedades de la información: confidencialidad, integridad, disponibilidad, autenticidad, no repudio, trazabilidad. Como la información puede estar contenida en diferentes soportes, medios, formas y no sólo en medios informáticos, aquí podemos citar como ejemplos documentación en papel, mobiliarios con diferentes documentos en su interior, y el recurso humano que es el activo de información más importante dentro de las organizaciones.

En síntesis, la seguridad de la información abarca la seguridad informática.

Figura 1: Seguridad de la información y seguridad informática

Activo de información

Un activo de información, es todo aquello que tiene un valor para la organización, pero que al mismo tiempo almacena y manipula información. Por ejemplo, una cajonera con expedientes en su interior, debe ser considerado un activo de información y, como tal, debe protegerse. En cambio una cajonera vacía, no representa un activo de información para la organización, sino un bien de uso. Es fundamental tener en claro este concepto para darles la protección adecuada a estos activos.

La información posee ciertas propiedades que definiremos a continuación:

- confidencialidad: es la propiedad de la información por la que se garantiza que sólo esta accesible por el personal autorizado.
- integridad: es la propiedad de la información por la que se garantiza que la misma no ha sido alterada.
- disponibilidad: es la propiedad de la información por la que se garantiza que está disponible siempre y cuando se la requiera.
- autenticidad: es la propiedad de la información por la que se garantiza la veracidad y exactitud de la misma.
- no repudio: es la propiedad de la Información por la que se garantiza la autoría de la misma.
- trazabilidad: es la propiedad de la información por la que se garantiza quién hizo qué y cuándo lo hizo.

Estos conceptos son fundamentales a la hora de identificar nuestros activos de información y realizar un análisis con respecto a todas sus propiedades, para decidir el nivel de protección adecuado que se necesita.

Los activos de información se deben inventariar en un documento llamado Inventario de activos de información. Para que este último sea transparente y entendible se pueden discriminar en diferentes categorías. Por ejemplo:

- Datos: todos aquellos datos que, en cualquier formato, se generan, se recogen, se gestionan, se transmiten y se destruyen.
- Aplicaciones: el producto de software que se utiliza para gestionar la información.
- Personal: todos aquellos que tengan acceso de una u otra forma a los activos de información.

- Servicios: servicios internos como externos.
- Tecnología: los equipos que se utilizan para gestionar la información y las comunicaciones.
- Equipamiento Auxiliar: son aquellos activos que dan soporte a los sistemas de información y que no están incluidos en ninguna de las categorías anteriores. Ejemplos de esto último son equipos de destrucción de datos, equipos de climatización, etc.

Cada activo debe contar con un responsable del mismo, quien será su propietario. Cuando mencionamos la palabra propietario, no queremos decir que tiene propiedad sobre el activo, sino responsabilidad sobre el mismo. Este propietario es quien se encargará de definir qué nivel de seguridad necesita el activo de información, quién accede a él y quién no, si existe algún riesgo que debe tenerse en cuenta, etc.
El Inventario de activo de información debe estar confeccionado de manera clara, ya que es la base para gestionar la información, mantenerla operativa, incluso recuperarse ante un desastre. Como mínimo el Inventario de activos de información debe tener:

- Identificación del activo: cualquier ID o identificador.
- Tipo: cualquiera de las categorías anteriormente mencionadas.
- Descripción: breve descripción clara del Activo.
- Propietario: responsable del Activo.
- Localización: dónde está físicamente el activo, en el caso de información electrónica o en digital, en que equipo o dispositivo se encuentra.

No se recomienda que el inventario de activos de información sea exhaustivo. Llevar este documento a nivel de detalle o desglosar los activos a nivel de registro dificultaría identificar las vulnerabilidades, las amenazas, por lo que haría mucho más difícil el análisis de riesgos.
Ni bien tengamos identificados todos los activos de información, lo siguiente que hay que hacer es valorizarlos.

Valorización y clasificación de los activos de información

La valorización indica cuál es la importancia que tienen para la organización y cuál sería el daño para la organización si el activo es vulnerado en cuanto a su confidencialidad, integridad y disponibilidad. Esta valorización se puede elaborar de manera cuantitativa como cualitativa. Es decir, si podemos valorar económicamente en el caso de la cuantitativa, o si utilizaremos una escala cualitativa como puede ser Alto, Medio, Bajo. Independientemente de la escala utilizada, los aspectos a considerar puede ser los daños respecto de:

- Violación de la legislación vigente (Marco Legal)
- Reducción del rendimiento de actividad
- Efecto negativo en la imagen
- Pérdidas económicas
- Problemas en el negocio

La valorización debe ser lo más objetiva posible. Esta valorización se lleva a cabo en base a las tres propiedades de la información mencionadas: confidencialidad, integridad y disponibilidad.
Para valorar la disponibilidad, se debe responder a la pregunta siguiente: ¿cuál sería la importancia o el "trastorno" si el activo de información no estaría disponible? Por ejemplo, si consideramos una escala de 0 a 3 se podría valorar de la siguiente manera:

Valor	Criterio
0	No aplica o no es relevante
1	Debe estar disponible al menos el 10 % del tiempo
2	Debe estar disponible al menos el 50 % del tiempo
3	Debe estar disponible al menos el 99 % del tiempo

Tabla 1: Valorización de la disponibilidad

Para valorar la integridad, la pregunta que habría que hacerse es ¿qué importancia tendría si el activo de información fuera alterado sin autorización ni control? Por ejemplo, se podría valorar de la siguiente forma:

Valor	Criterio
0	No aplica o no es relevante
1	No es relevante los errores que tenga o la información que falte
2	Tiene que estar correcto y completo al menos en un 50 %
3	Tiene que estar correcto y completo al menos en un 95 %

Tabla 2: Valorización de la integridad

Para valorar la confidencialidad, la pregunte que habría que hacerse es ¿qué importancia tendría que el activo de información tenga un acceso no autorizado? Por ejemplo, aquí la escala podría ser:

Valor	Criterio
0	No aplica o no es relevante
1	Daños muy bajos, el incidente no transcendería del área afectada
2	Serían relevantes, el incidente implicaría a otras áreas
3	Los daños serían catastróficos, la imagen y reputación de la organización se verían afectados

Tabla 3: Valorización de la confidencialidad

Luego hay que decidir cómo valorar totalmente a los activos de información. Una buena forma sería que, a partir del valor de cada parámetro analizado, se designe de manera subjetiva la forma en que el activo en cuestión responde a los objetivos del alcance del Sistema de Gestión de la Seguridad de la Información (SGSI) sobre el cual trataremos más adelante. Es decir, si cumple ampliamente con los objetivos del proceso se puede valorar como alto, si cumple medianamente con los objetivos se puede valorar como medio y si

finalmente no incide en los objetivos del Alcance o no es relevante, se puede valorar como bajo.

Fallo de seguridad

Un fallo de seguridad es cualquier incidente que la compromete, es decir que pone en peligro cualquiera de las propiedades de la información descriptas anteriormente. Como ejemplo de fallo de seguridad, podemos citar: fallos en el suministro eléctrico, fallos en las comunicaciones, fallos humanos (ya sean internos como externos a la organización), fallos en los sistemas de información, códigos maliciosos, accesos no autorizados o incumplimiento de leyes o reglamentos.
Los fallos de seguridad a menudo suceden porque se tiene la errónea percepción de que si la seguridad física está asegurada no debería haber mayores inconvenientes. O porque tenemos asegurado todo lo referente a la seguridad informática. Pero de esta manera se deja sin protección muchas áreas y muchos activos de información pueden ser dañados o destruidos por no considerar todos los aspectos de seguridad de la información.
Para entender un poco más este punto debemos saber que existen amenazas potenciales, que pueden explotar vulnerabilidades de nuestros activos de información produciendo riesgos, y de esta forma tendremos un impacto determinado sobre nuestro negocio. A continuación describiremos los criterios de la información sobre estos puntos:

- Amenaza: evento que puede comprometer un activo de información.
- Vulnerabilidad: debilidad que hace susceptible a un activo de información.
- Riesgo Intrínseco: nivel de riesgo sin ningún tipo de control aplicado al mismo.
- Riesgo Residual: nivel de riesgo resultante una vez aplicados los controles.
- Impacto: resultado de la materialización de la amenaza.

Análisis y valorización de los riesgos

El análisis de riesgos es una de los puntos clave. Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o varios activos de información causando daños o perjuicios a la organización. El riesgo nos indica qué sucedería si no se protegen adecuadamente los activos. El análisis de riesgos se define como la utilización sistemática de la información disponible, para determinar los peligros y estimar los riesgos.
Es fundamental ajustarse a las necesidades y los recursos de la organización para que se puedan cubrir las expectativas, llegando al nivel de seguridad requerido con los medios disponibles. Es más sencillo calcular con cuantos recursos se cuenta, pero no es tan fácil saber ciertamente las necesidades de seguridad.
Por eso mismo es importante la realización de un análisis de riesgos, porque permite averiguar cuáles son los peligros a los que se enfrenta la organización y la importancia de cada uno de ellos. Con esta información podemos hacer una toma de decisiones bien fundamentada acerca de qué medidas de

seguridad deberían implantarse. Por lo tanto, un aspecto de gran importancia es tener en cuenta que la inversión en seguridad debe ser proporcional al riesgo.
Para realizar el análisis de riesgos, se debe partir del inventario de activos. Si este último no es extenso, se puede decidir hacer el análisis de riesgos sobre todos los activos de información involucrados. Si por el contrario es muy extenso, es más recomendable agrupar los Activos de Información, decidiendo esto sobre los que tienen más valor, o los que son más estratégicos.
En el análisis de riesgos, vamos a valorar todas las amenazas identificadas que pueden afectar a nuestros activos de información, identificaremos las vulnerabilidades que podrían explotar dichas amenazas y el impacto que causaría en caso de que alguna amenaza se materialice. Por lo tanto el análisis de riesgo es bastante laborioso.
Independientemente de la Metodología que se utilice para realizar el análisis de riesgos, se puede abordar el mismo con varios enfoques dependiendo del grado de profundidad con que se quiera realizar el análisis. Dichos enfoques puede ser:

- Enfoque de Mínimos: se escoge un conjunto mínimo de activos de información y se hace un análisis conjunto, de manera que se emplean una cantidad mínima de recursos, consumiendo menos tiempo y con un costo menor. Este enfoque tiene la desventaja de que puede ser difícil actualizar los controles o añadir otros según vayan dándose cambios significativos.
- Enfoque Informal: aquí no se necesita una formación especial ni tantos recursos de tiempo ni personal. Las desventajas son que al no estar basado en métodos estructurados, puede suceder que se pasen por alto riesgos o amenazas importantes y al depender de las personas que los realizan, el análisis puede resultar con cierto nivel de subjetividad. Si no se argumenta bien la selección de controles, puede ser difícil después justificar el gasto de implantación.
- Enfoque Detallado: con este enfoque se consigue una idea muy exacta y objetiva de los riesgos a los que se enfrenta la organización. Se puede decidir un nivel de seguridad apropiado para cada activo de información y de esa forma escoger los controles con precisión. Es el enfoque que más recursos necesita en tiempo, personal y dinero para llevarlo a cabo.
- Enfoque Combinado: con un enfoque de alto nivel al principio, permite determinar cuáles son los activos de información en los que habrá que invertir más antes de utilizar muchos recursos en el análisis. De esta manera ahorra recursos al tratar antes y de manera exhaustiva los riesgos más importantes mientras que al resto de los riesgos sólo se les aplica un nivel básico de seguridad, con lo que se consigue un nivel razonable de seguridad con recursos ajustados. Es el enfoque más eficaz en cuanto a costos y adaptabilidad a empresas chicas, Pymes, ONG.

Con todo esto, podemos identificar las amenazas, las vulnerabilidades que dichas amenazas podrían explotar y el impacto en caso de que se materialicen. Esto nos permite identificar los riesgos y cuáles deben ser tratados primero o con más detalle. Se debe escoger cual es el nivel de riesgos que la organización está dispuesta a tolerar. De esta manera, debajo de ese nivel el riesgo será aceptable, pero por el contrario si el mismo está por encima de dicho nivel, se deberá tomar alguna decisión al respecto.
Sobre los riesgos no aceptables, hay 4 tipos de decisión que podemos tomar:

- Transferirlo: el riesgo se traspasa a otra organización, por ejemplo una Compañía de Seguros.
- Eliminarlo: está decisión no suele ser viable, ya que eliminar el riesgo significa eliminar el activo de información que lo genera.
- Mitigarlo: reducir el riesgo, normalmente aplicando controles de seguridad.
- Aceptarlo: aceptar que no se puede hacer nada y por lo tanto, se acepta ese riesgo, pero la organización sabe que existe.

Toda esta información debe quedar documentada para justificar las acciones que se van a tomar en cuanto a los riesgos y conseguir el nivel de seguridad aceptado por la organización.
Existen diferentes metodologías para realizar el análisis de riesgos, ya que es un trabajo bastante estructurado y con una metodología se facilita bastante. Se debe escoger aquella que se ajuste mejor a las necesidades de la Organización. Algunas de las metodologías disponibles son las siguientes:

- ANÁLISIS HOLANDES A&K: desarrollada por el Ministerio de Asuntos Internos de Holanda, hay publicado un manual y se usa en el Gobierno y en empresas holandesas.
- CRAMM: desarrollado por el Gobierno Británico y cuenta con una herramienta ya que es un método difícil de utilizar sin ella.
- EBIOS: es un juego de guías mas una herramienta de código libre gratuita, enfocada a gestores del riesgo TI.
- IT-GRUNDSCHUTZ: desarrollada en Alemania por la Oficina Federal de seguridad de la información, proporciona un método para establecer un SGSI en cualquier organización.
- MAGERIT: desarrollada por el Ministerio de Administración Pública de España, describe los pasos para la realización de un análisis de riesgos y la gestión para mitigarlos.
- NORMA ISO/IEC 27005: la norma habla de la gestión de riesgos de manera genérica, utilizando el modelo PDCA o Círculo de Deming.

Sistema de gestión de la seguridad de la información

Hasta el momento, lo más común es ir “parcheando” los “agujeros” de seguridad con medidas puntuales, las cuales son descoordinadas, y pocos proporcionados en relación al riesgo que reducen. Estas medidas son llevadas a cabo sin ningún tipo de planificación, y el resultado es nada más ni nada menos que mantener el mismo nivel de riesgo frente a las amenazas.

Todos estos incidentes que amenazan la seguridad de la información requieren de sistemas de gestión acordes con el valor de la propia información. Las directrices, procedimientos y controles de seguridad es lo que se conoce como Sistema de Gestión de seguridad de la información, a partir de ahora SGSI. Con este tipo de sistemas, nos aseguraremos de cubrir todos los aspectos de seguridad tomando medidas adecuadas con el fin de reducir los riesgos a los que está expuesta la organización.
Un SGSI no debe ser considerado ni un costo ni tampoco un esfuerzo relevante, dado los beneficios que conlleva. Debe ajustarse a las necesidades del negocio como a los recursos disponibles, solucionando los problemas pero siempre dentro de un marco de coherencia en cuanto a costos y esfuerzos. Como cualquier otro sistema de gestión, un SGSI debe ayudar a conseguir los objetivos de la organización sin convertirse en un impedimento para ello.
El SGSI identifica los objetivos que se pretenden conseguir y los medios con los que se cuentan para ello. Para determinar ambas cosas se debe realizar un análisis de riesgos que nos dé la pauta de hasta qué medida los activos de información están expuestos a que les ocurran fallos de seguridad y cuál sería el impacto en caso de que ocurriesen. Con esta información tendremos el punto de partida, es decir, en qué estado esta nuestra seguridad de la información, y se deberá definir cuál es el estado pretendido, así como el objetivo para dentro de un plazo de tiempo determinado.
A partir de esto lo expuesto, definiremos un SGSI como la forma en que la organización conoce los riesgos a los que está expuesta su información y los gestiona de una forma sistemática, documentada y conocida por todos, que se revisa y mejora continuamente.

Beneficios e importancia de la seguridad en el negocio

Muchas Pymes u otras organizaciones pequeñas tienen que confrontar hoy en día con las limitaciones de presupuesto, la falta de concientización y sobre todo de conocimientos para enfrentar nuevos retos. La seguridad abarca mucho lo tecnológico, a partir de eso se la toma como un área diferente, que queda en manos de expertos, generalmente tercerizados, los cuales no conocen bien nuestro negocio.
La seguridad de la información está ligada directamente con la “supervivencia del negocio” y la protección de los ingresos. Para una Pyme, por ejemplo, sería muy problemática un fallo de energía que dure un tiempo de unas horas, con repercusiones económicas, ya que se interrumpe la actividad.
Con el avance tecnológico, donde una computadora sustituye a la máquina de escribir y el correo electrónico sustituye al tradicional, vienen aparejados los diferentes peligros que acompañan a estos avances. Son riesgos que generalmente no se contemplan. De esta forma el negocio corre un peligro mayor.
Un proyecto de seguridad de la información no significa un costo. Por el contrario, contar con un sistema de gestión permite ordenar las actividades para que sean dirigidas al objetivo propuesto por la organización. Por lo tanto, un SGSI es un proyecto rentable tanto para organizaciones pequeñas como para grandes organizaciones.
Los beneficios más sobresalientes de contar con un SGSI son:

- Reducción de costos
- Optimizar los recursos

- Protección del negocio
- Mejor competitividad
- Cumplimiento marco legal y reglamentario
- Mantener y mejorar la imagen corporativa

Marco legal de la Argentina en materia de seguridad de la información

Estas leyes se han creado para protegernos de los delitos informáticos. Un delito de este tipo es todo ilícito digital que implique la utilización de cualquier medio de tecnología informática.
La legislación argentina en materia de seguridad de la información incluye las siguientes normativas:

- Ley N° 24.766.- Confidencialidad
- Ley N° 25.036.- Modificatoria de la Ley N° 11.723.- Propiedad Intelectual
- Ley N° 25.188.- Ética en el ejercicio de la función pública
- Ley N° 25.326.- Protección de Datos Personales
- Ley N° 25.506.- Firma Digital
- Ley N° 25.520.- Inteligencia Nacional
- Ley N° 26.388.- Delitos Informáticos. Modificación al Código Penal.
- Decisión Administrativa 669/04.- Políticas de seguridad de la información

Estándares de seguridad de la información

El principal estándar aceptado en el área de seguridad de la información corresponde a la familia de las Normas ISO 27000. ISO (*International Standard Organization,* Organización Internacional de Estándares), es una organización especializada en el desarrollo y difusión de estándares a nivel mundial.
Sus miembros son organismos nacionales que participan en el desarrollo de normas internacionales a través de Comités Técnicos establecidos para tratar cada campo en particular. En el caso de la familia de las ISO 27000, colabora la IEC (Comisión Internacional Electromecánica), que prepara, coordina y publica a nivel mundial estándares en el campo de la electrotecnología.
Al igual que la familia de las ISO 9000, estándar aceptado a nivel mundial en el campo de la calidad, la familia de las ISO 27000 es también una serie de estándares cuya estructura está definida de la siguiente manera:

- ISO/IEC 27000: SGSI. Conceptos y generalidades
- ISO/IEC 27001: SGSI. Requisitos
- ISO/IEC 27002: Código de buenas prácticas para la gestión de la seguridad de la información
- ISO/IEC 27003: Guía de implementación de un SGSI. Circulo de Deming o PDCA (Planificar, Hacer, Checkear, Actuar). Ciclo de mejora continua.
- ISO 27004: Métricas. Medición efectividad controles.

- ISO/IEC 27005: Metodología para la Gestión del Riesgo
- ISO/IEC 27006: Requisitos para entidades de servicio de Auditoría y Certificación de SGSI
- ISO/IEC 27007: Guía para la realización de Auditorías de un SGSI
- ISO/IEC 27011: Directrices para la seguridad de la información en organizaciones de Telecomunicaciones utilizando la Norma ISO/IEC 27002
- ISO/IEC 27799: Gestión de la seguridad de la información sanitaria utilizando la Norma ISO/IEC 27002

La Norma ISO/IEC 27001 es la única certificable de la serie.
Estas son normas de gestión que se aplican a cualquier tipo de organización y son independientes al tamaño de la misma, a su tipo o actividad. Están basadas en procesos y en la mejora continua, por lo tanto son perfectamente adaptables al resto de los sistemas de gestión que ya estén en marcha en la organización. Otro punto a tener en cuenta es que si bien se puede comenzar certificando la organización en su totalidad, esto no es aconsejable. Se aconseja ir implementando y certificando por ámbitos y el proceso de certificación no debería superar el año, ya que si no se corre el riesgo que lo efectuado en un principio quede obsoleto.
Por último, cabe aclarar que sería un error tratar de seguir las indicaciones que se dan como si fuera una receta de cocina, o bien al pie de la letra. Muchas pueden ser muy complejas y no adaptarse a la organización, por lo que no hay que descuidar la cultura organizacional en este aspecto. Por ejemplo, un SGSI que funciona perfectamente en la Organización “A” seguramente no funcionaría igual de bien en la Organización “B”, pues el SGSI debe adaptarse a la cultura que tenga cada organización en particular. Esto se logra con capacitación y concientización.

Ç

Implementación de un SGSI siguiendo el Círculo de Deming

El Círculo de Deming es un ciclo de mejora continua para la implantación de un Sistema de Gestión compuesto por cuatro etapas: planificar (*plan*), hacer (*do*), comprobar (*check*) y actuar *(act)*.

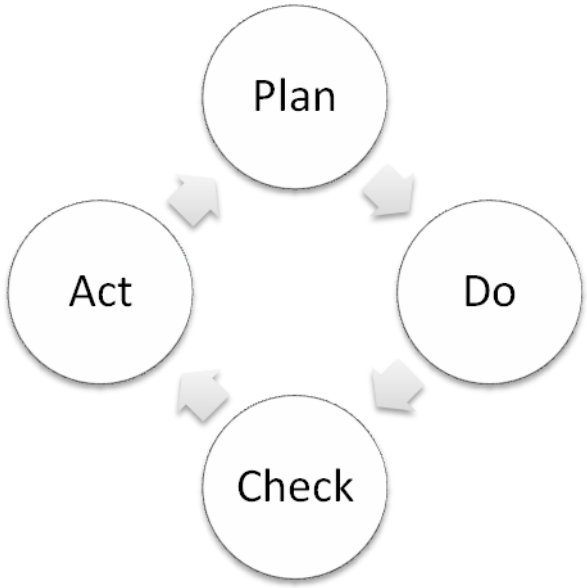

Figura 2: Arquitectura del Círculo de Deming o PDCA. Ciclo de Mejora Continua.

Fase Plan. Planificar y diseñar el SGSI según la Norma ISO/IEC 27001.
Establecer el alcance del SGSI. Es decir, qué parte de la organización se va a proteger.
Establecer las responsabilidades. Se designará a un responsable de seguridad quien coordinará las tareas en materia de seguridad. El área de seguridad deberá ser totalmente independiente, un staff como Organización y Métodos en el área de calidad. También es recomendable designar un Comité de seguridad de la Información que trate y busque soluciones en los temas de seguridad, resuelva los asuntos interdisciplinarios, y apruebe las normas y directrices
Definir la política de seguridad de la información. Dicha política debe ser sencilla, corta y entendible por cualquier persona de la Organización. Debe ser pública, es decir disponible para todo el personal, y debe definir qué pretende la organización en cuanto a seguridad de la información. Aquí es donde se va a mostrar un factor fundamental para la implantación de un SGSI, que es el compromiso de la Alta Dirección.
Realizar un análisis de riesgos. Es la actividad que nos dará la visión de los principales problemas actuales o potenciales que se deben solucionar para alcanzar el nivel de seguridad deseado. Debe ser proporcionado a la valoración de los activos de información y de los riesgos a los cuales dichos activos están expuestos. La valoración del riesgo debe identificar las amenazas que puedan explotar vulnerabilidades de los activos de Información, su impacto en la organización, determinando así el nivel de riesgo.

Seleccionar los controles. Una vez que sabemos dónde se encuentran los puntos débiles gracias a la gestión de riesgos, debemos escoger los controles para reducir esos riesgos.
Establecer el plan de seguridad. Es un plan con los plazos, recursos y prioridades.

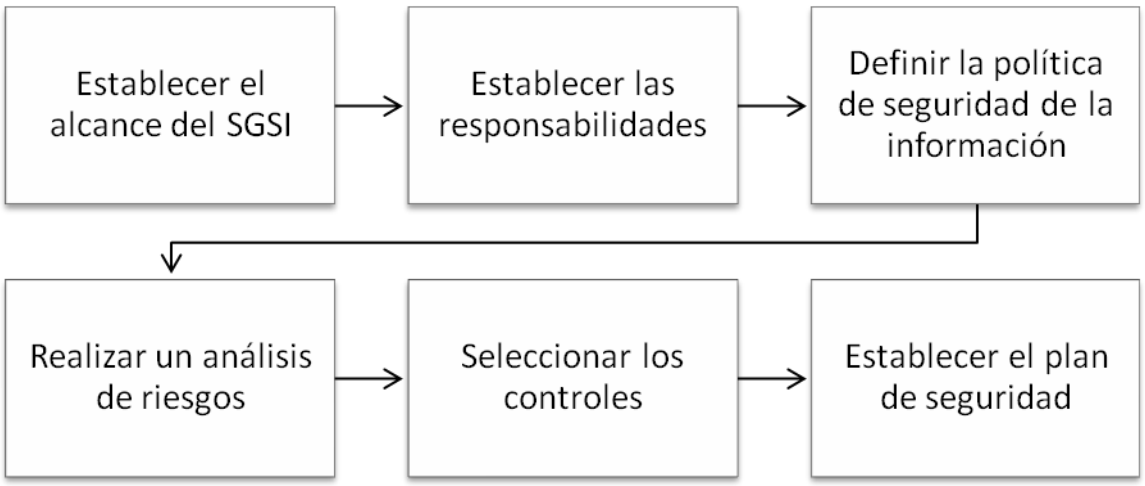

Figura 3: Actividades de la etapa de Plan

Fase Do. Hacer.
Aquí se lleva a cabo el Plan de Seguridad definido en la anterior fase. Los principales documentos a generar son:

- Política de seguridad de la información: que indica lo que busca la organización en cuanto a seguridad.
- Inventario de Activos de Información: descripción y valoración de los activos de información
- Declaración de Aplicabilidad: por cada control del mencionado Anexo A de la Norma, cual aplica y cual no, justificando tanto selección como exclusión de los mismos
- Procedimientos: procedimientos documentados de las tareas a realizar para la ejecución de los controles
- Registros: son la evidencia de que se han realizado las tareas del SGSI. Son fundamentales a la hora de medir la eficacia de las medidas implantadas

Una tarea importante en esta fase es la capacitación y concientización, factores fundamentales nombrados anteriormente. Todo el personal debe saber que se está haciendo y para qué se está haciendo, concientizando a todas las personas de nuestra organización sobre las buenas prácticas en materia de seguridad de la información.

Fase Check. Comprobar.
Una vez puesto en marcha el plan de seguridad, se debe revisar periódicamente de manera que se detecten posibles no conformidades. Una no conformidad es el incumplimiento de un requisito, que puede ser propio de la norma, legal, etc. Pueden surgir problemas imprevistos y que deben ser solucionados para continuar con el plan.
Otra de las comprobaciones que se deben realizar es la auditoría interna. El objetivo de la misma es evaluar la eficacia de los controles implementados, procesos y procedimientos. Se determinará:

- Están conformes con los requisitos de la Norma ISO/IEC 27001
- Están conformes con la legislación vigente
- Están conformes con los requerimientos de seguridad identificados
- Están implementados y mantenidos de manera efectiva
- Dan el resultado esperado

Si se detectan No Conformidades, se deben tomar las medidas necesarias para corregirlas.

Fase Act. Actuar.
Cuando se detectan no conformidades, se debe actuar en consecuencia para corregirlas. Hay tres formas para hacerlo:

- Adoptar acciones correctivas: son acciones que se toman para corregir no conformidades significativas con los requisitos del SGSI.
- Adoptar acciones preventivas: son aquellas que se toman para evitar que ocurra algo no deseado. La gran ventaja aquí es que es más fácil prevenir problemas que solucionarlos.
- Definir acciones de mejora: estas acciones surgen a partir de la dinámica del SGSI. Impulsa a refinar procesos y superar objetivos continuamente.

Políticas, organización, alcance y concientización

Política de seguridad de la información.
El objetivo de la política de seguridad de la información es dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo a las necesidades del negocio y a la legislación vigente. Es un requisito de la Norma ISO/IEC 27001. Este documento lo define la Alta Dirección, estableciendo qué busca la organización en cuanto a seguridad de la información de forma clara, corta y concisa, considerando que debe estar alineado a los objetivos del negocio. La política de seguridad de la información es también una forma de manifestación expresa del apoyo y compromiso que asume la Alta Dirección en materia de seguridad de la información. Esto último es fundamental para que todo el personal de la organización perciba la importancia de la temática. Como se mencionó anteriormente, la política de seguridad de la información debe ser comprensible y estar disponible para todo el personal de la organización.

Organización de la seguridad de la información.
Corresponde a los aspectos organizativos de la seguridad de la información y trata la seguridad interna como así también la relación de la organización con terceras partes (clientes, proveedores, etc.). A veces se añadirán responsabilidades a puestos existentes, como así también puestos nuevos. En organizaciones pequeñas, como Pymes y ONG, los nuevos puestos es recomendable que sean asumidos por recursos humanos propios. Hay dos funciones principales; un responsable de seguridad, quien coordinará todas las tareas en materia de seguridad de la información, e integrantes del Comité de seguridad de la información, quienes trataran los problemas de seguridad, discutirán las soluciones a los mismos, identificarán no conformidades, cambios significativos, valorarán si los controles implantados son suficientes y coordinarán la implantación de nuevos controles, revisarán y aprobarán directrices y normas, marco legal.

Alcance del SGSI
Aquí hay que definir que ámbito de la organización se va a proteger, si es que no se decide abarcar toda la organización. La Norma ISO recomienda comenzar por un determinado ámbito. Una vez decidido esto, se debe definir claramente el alcance del SGSI teniendo en cuenta las localizaciones físicas incluidas, las actividades de la organización, las tecnologías utilizadas, etc. Definir el alcance del SGSI es uno de los puntos críticos ya que su correcta definición hará que las tareas de implantación y los responsables estén correctamente establecidos y de esta manera se facilita la mantención con los recursos disponibles y las necesidades de la organización.

Concientización.
Esta es una parte fundamental. Aquí se debe educar a todo el personal de la organización, esté involucrado directamente o no en el proyecto, en materia de seguridad de la información. Todo el personal debe saber qué se está haciendo y por qué se está haciendo. Se deben llevar a cabo tareas de divulgación de buenas prácticas, para que el personal vea de manera transparente los cambios que se avecinan. También se debe definir un plan de formación, establecer cuáles son las necesidades dentro de ese plan, y tomar las acciones necesarias para cubrirlas. Este plan no debe ser encaminado a través de cursos externos costosos, sino que hay que analizar con qué recursos disponibles contamos para llevarlo a cabo. Es viable la contratación de alguna persona externa a la organización que cuente con las competencias necesarias para ejecutar el plan de formación. Muy importante es llevar un registro donde se puedan recolectar evidencias de la ejecución del plan. El resultado final de esta formación debe ser la apertura a una modificación de la cultura organizacional que conllevará el compromiso en las labores relativas a la seguridad de la información como parte de la “vida laboral cotidiana” y sobre todo, como un todo en la organización.

Seguimiento, monitorización y registro de las operaciones del sistema

Una vez que conocemos los riesgos a los que está sometida la organización y tomamos las decisiones y se implementan los controles necesarios para conseguir un nivel de riesgo aceptado por la organización, se debe hacer un seguimiento de cómo funciona el sistema para corregir las posibles desviaciones sobre lo planificado y al mismo tiempo identificar oportunidades de mejora. Esto es así ya que el objetivo fundamental es perseguir la mejora continua.
La Alta dirección debe realizar una revisión continua del sistema, como mínimo anual. Esta revisión forma parte de la Fase CHECK del modelo PDCA o Círculo de Deming. Aquí se chequea todo el funcionamiento del Sistema de Gestión de seguridad de la información, se detectan las no conformidades respecto a lo planificado como así también las oportunidades de mejora, y se actúa en consecuencia (como parte de la fase Act), comenzando luego nuevamente el circuito con la fase Plan.

Ejemplo práctico de Plan de Contingencia o de Continuidad del Negocio mediante una Metodología Cualitativa para la Evaluación de Riesgos basada en la Norma ISO/IEC 27005:2013.-

Si bien esta Metodología es propietaria y se utiliza en el marco de un proceso de certificación bajo la Norma ISO/IEC 27001:2013,- no está mal utilizarla para la confección de planes estratégicos como de contingencias o de continuidad del negocio. Si bien se suelen utilizar estos dos términos como si fueran un común denominador, es necesario saber que existe una pequeña pero fundamental diferencia. El nombre del plan se determinará según el requerimiento del negocio. Es decir, si mi proceso o ámbito de aplicación no consta de una característica como ser sensible o crítico, puedo optar por un plan de contingencias para tener capacidad de respuesta justamente ante contingencias determinadas que se puedan presentar. En cambio si por el contrario mi proceso o ámbito de aplicación si es crítico o sensible, puedo optar por un plan de continuidad del negocio, ya que necesito recuperarme lo antes posible ante contingencias determinadas que se puedan presentar y paren la operatoria del negocio.
Por lo tanto el formato del plan no varía, pero si el tratamiento estratégico.
Comenzando con el ejemplo práctico, lo primero que necesito saber es el Alcance de aplicación y su delimitación. Lo mejor para determinar esto, es pensar en procesos y realizarlo mediante un Diagrama de Flujo o Flujograma. En el ejemplo trataremos un proceso sencillo de Atención a Clientes de un Call Center.

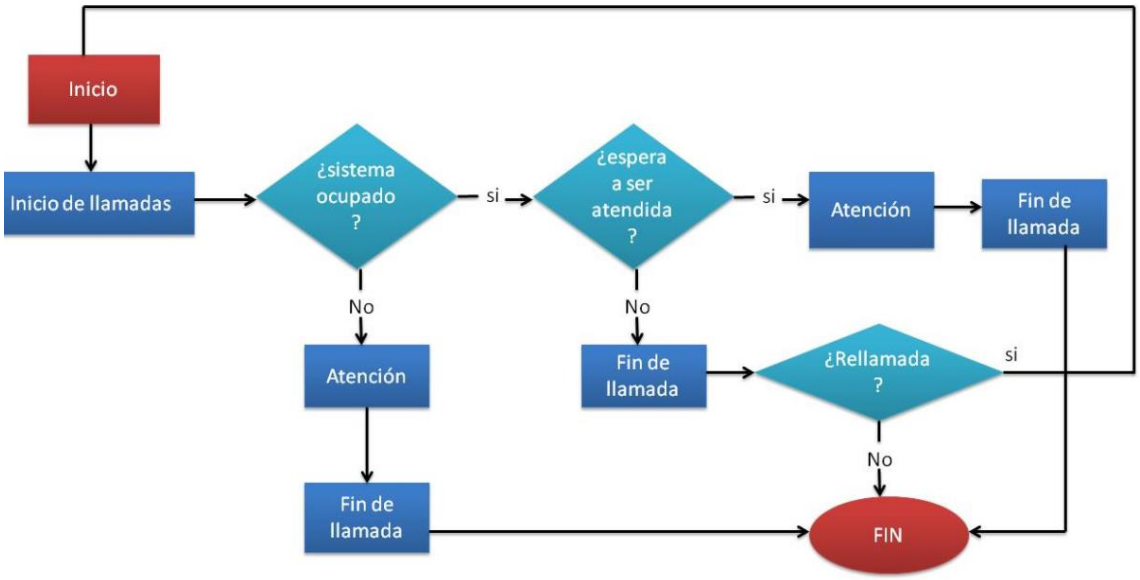

Figura 4: Flujograma Proceso Atención a Clientes de un Call Center.

Mediante el ejemplo, podemos determinar que el Alcance es el proceso de atención a clientes, cuyo Límite es desde la canalización de los reclamos, consultas, sugerencias hasta la resolución de las mismas. Cabe aclarar que vamos a suponer que en el mencionado proceso se realizan todas las acciones necesarias como registros y evidencias, necesarios y fundamentales para llevar a cabo nuestra tarea. En la práctica, esto no siempre es así, por lo tanto se necesita realizar todo lo necesario para comenzar con la generación de registros y evidencias, cuyo plazo mínimo de recolección recomendable para comenzar a trabajar es de tres meses.

Lo siguiente que debemos hacer es inventariar todos los activos de información dentro del Alcance determinado. Es decir, todo aquello que representa un valor para el mismo. Este trabajo se debe realizar en conjunto con los propietarios de cada activo, ya que son ellos quienes los tratan a diario, dando un mejor resultado para luego clasificarlos y darles un valor. Este primer documento, llamado inventario de activos de Información, es el punta pie inicial en el trabajo de evaluar riesgos. El mismo deberá contener como mínimo ID del activo, denominación, breve descripción, propietario.
En nuestro ejemplo, el inventario será:

ID	Activo	Descripción	Propietario
1	Central Telefónica	Comunicación	Depto. Telecomunicaciones
2	Servicio Telefónico	Comunicación	Proveedor
3	Servicio Eléctrico	Electricidad	Proveedor
4	Registros de Gestión	Consultas, sugerencias, reclamos.	Depto. Atención a Clientes
5	RR.HH.	Personal	Gerencia de RR.HH.
6	Lugar Físico	Ámbito laboral	Depto. Servicios Generales
7	Sistema de Aplicación	Software aplicativo	Depto. Análisis y Desarrollo
8	Correo Corporativo	E-Mail	Depto. Atención a Clientes
9	Equipamiento Informático	PCs, impresoras	Depto. Tecnológia
10	Información Digital	Información en formato o soporte electrónico	Depto. Atención a Clientes
11	Información en papel	Información en formato papel o tangible	Depto. Atención a Clientes
12	Instalación Eléctrica	Infraestructura eléctrica	Depto. Electricidad
13	Instalación de Datos	Infraestructura de Datos	Depto. Telecomunicaciones
14	Identidad Clientes	Validación	Depto. Atención a Clientes

Tabla 4: Inventario de Activos de Información.

Cabe aclarar que para reconocer al propietario de cada activo, es necesario el organigrama de la organización para determinar la propiedad, es decir el responsable del activo.
Estos serían los activos más básicos dentro del ejemplo, y de esta manera quedan inventariados para su identificación. Luego pasaremos a clasificar cada activo, y lo realizaremos en cuanto a su confidencialidad, integridad y disponibilidad. Utilizaremos de escala la vista en donde explicamos todo lo referente a Activos de Información, de 0 a 3.-

Cabe aclarar que la clasificación se realiza tal lo explicado anteriormente sobre los activos de información. Aquí debemos preguntarnos qué pasa si hay un acceso no autorizado en el caso de la confidencialidad, qué pasa si existe alguna alteración en el caso de la integridad y qué pasa si no está disponible en el caso de la disponibilidad. De esta manera sabremos qué nivel de seguridad necesita cada activo. De ahí la importancia de trabajar con los propietarios o responsables de los mismos. Ya que son ellos quienes saben

qué tipo de protección necesitan para sus activos. Si somos observadores, en nuestro proceso se destaca la integridad y la disponibilidad. Eso en nuestro caso es más que obvio, necesitamos que la información para el caso de Atención a Clientes sea integra y esté disponible. En el caso de un Banco, por ejemplo, se destacaría la confidencialidad en una eventual clasificación de activos, ya que se manejan datos de clientes y en muchos casos datos personales, críticos y sensibles ante un acceso no autorizado.
Para continuar con nuestro trabajo, ahora debemos valorizar los activos de información. Para ellos utilizaremos una escala del tipo Alto, Medio, Bajo. Esto es en relación activo de información – objetivo de proceso. Es decir la importancia del activo en cuanto al Alcance determinado .En la Tabla siguiente(5) se observa la clasificación de Activos.

iID	Activo	Confidencialidad	Integridad	Disponibilidad
11	Central Telefónica	2	3	3
12	Servicio Telefónico	1	3	3
13	Servicio Eléctrico	1	3	3
14	Registros de Gestión	3	3	3
55	RR.HH.	2	3	3
66	Lugar Físico	2	3	3
77	Sistema de Aplicación	2	3	3
88	Correo Corporativo	2	3	3
99	Equipamiento Informático	2	3	3
110	Información Digital	2	3	3
111	Información en Papel	2	3	3
112	Instalación Eléctrica	1	3	3
113	Instalación de Datos	1	3	3
114	Identidad Clientes	2	3	3

iID	Activo	Valor (A; M; B)
11	Central Telefónica	A
22	Servicio Telefónico	A
33	Servicio Eléctrico	A
44	Registros de Gestión	A
55	RR.HH.	A
66	Lugar Físico	M
77	Sistema de Aplicación	A
88	Correo Corporativo	A
99	Equipamiento Informático	A
110	Información Digital	A
111	Información en Papel	A
112	Instalación Eléctrica	A
113	Instalación de Datos	A
114	Identidad Clientes	A

Tabla 6: valorización de Activos de Información.

Una vez valorizados todos los activos de información para el Alcance del ejemplo, estamos en condiciones de comenzar con el Análisis y la Estimación del Riesgo. Este es un documentado donde identificaremos amenazas, vulnerabilidades con las probabilidades de ocurrencia y el impacto. Cabe mencionar y aclarar que esto se realiza siempre en base a registros y

evidencias, de forma cualitativa, como así también que en este ejemplo la relación activo-amenaza y amenaza-vulnerabilidad será del tipo 1 a 1 para simplificar el ejemplo, pero en la realidad la relación es 1 a muchos, es decir para un activo muchas amenazas y para una amenaza hay muchas vulnerabilidades. Para la probabilidad de ocurrencia y el impacto tomaremos una escala muy bajo, bajo, medio, alto, muy alto.
Continuamos con el ejemplo:

IID	Activo	Amenaza	Clasificación	P.O.	Vulnerabilidad	Impacto
11	Central Telefónica	Falla Central	Tecnológica	B	Falta de Mantenimiento	MA
22	Servicio Telefónico	Corte Suministro	Tecnológica	B	Falta Plan “B”	MA
33	Servicio Eléctrico	Corte Suministro	Tecnológica	B	Falta Plan “B”	MA
44	Registros de Gestión	Pérdida de Información	Operacional	B	Falta Copia de Resguardo	MA
55	RR.HH.	Divulgación de Información	Humana	B	Falta Acuerdo de Confiabilidad	A
66	Lugar Físico	Deterioro Edilicio	Física	MB	Falta de Mantenimiento	M
77	Sistema de Aplicación	Caída del Sistema	Tecnológica	B	Problema Hard/Soft	MA
88	Correo Corporativo	Código Malicioso	Tecnológica	M	Día Zero Código Malicioso	MA
99	Equipamiento Informático	Robo y Fuga de Información	Tecnológica	B	Sin bloqueo Puertos USB/ Acceso web a discos virtuales.	A
110	Información Digital	Pérdida de información	Tecnológica	B	Falta Copia de Resguardo	MA
111	Información en Papel	Pérdida de información	Operacional	B	Falta Política Pantalla y Escritorios Limpios	A

112	Instalación Eléctrica	Deterioro Infraestructura Cableado Eléctrico	Tecnológica	M	Falta Mantenimiento	A
113	Instalación de Datos	Deterioro Infraestructura Cableado de Datos	Tecnológica	B	Falta Mantenimiento	A
114	Identidad Clientes	Robo de Identidad	Operacional	B	Falta de Validación	MA

Tabla 7: Análisis y Estimación del Riesgo.

Una vez finalizado el documento anterior, estamos en condiciones de realizar la toma de decisión sobre el riesgo. Y para eso utilizaremos una tabla de criterio, donde utilizaremos todos los datos de los documentos confeccionados hasta ahora.
La tabla es la siguiente:

Valor Activo		BAJO					MEDIO					ALTO				
Impacto		MB	B	M	A	MA	MB	B	M	A	MA	MB	B	M	A	MA
P.O	MA															
	A															
	M															
	B															
	MB															

Tabla 8: Tabla de Criterio del Riesgo

Utilizando el valor obtenido de cada activo, posicionándonos en la parte superior de la tabla, nos ubicaremos en el sector correspondiente y nos ubicaremos en el eje cartesiano utilizando los valores obtenidos del Análisis y Estimación del Riesgo. Según el color del lugar de posicionamiento estratégico en la tabla tomaremos la decisión sobre el riesgo, para avanzar a la Gestión y Plan de Tratamiento del Riesgo. Esto es Rojo = Accionar lo antes posible,

Naranja = Mitigar o minimizar el riesgo, Amarillo = Transferir el riesgo y Verde = Aceptar el riesgo.

En la Gestión y Plan de Tratamiento del Riesgo estableceremos el cómo se va a tratar el riesgo, quién lo va a hacer, cuándo se va a hacer y con qué recursos, esto siempre según el criterio de decisión obtenido a través de la tabla (Ver Tabla 8).

Continuando con el ejemplo:

Activo de Información	Central Telefónica
Amenaza Identificada	Falla Central
Vulnerabilidad que podría explotar	Falta de Mantenimiento
Valor Activo de Información	A
Accionar	
Mitigar	X
Transferir	
Aceptar	
Cómo	Acuerdo de Nivel de Servicio
Quién	Depto. Telecomunicaciones
Cuándo	Diciembre 2017
Recursos	Propios

Activo de Información	Servicio Telefónico
Amenaza Identificada	Corte Suministro
Vulnerabilidad que podría explotar	Falta Plan “B”
Valor Activo de Información	A
Accionar	
Mitigar	X
Transferir	
Aceptar	
Cómo	Unidades Móviles de Resguardo
Quién	Depto. Telecomunicaciones
Cuándo	Diciembre 2017
Recursos	Propios

Activo de Información	Servicio Eléctrico
Amenaza Identificada	Corte Suministro
Vulnerabilidad que podría explotar	Falta Plan “B”
Valor Activo de Información	A
Accionar	
Mitigar	X
Transferir	
Aceptar	
Cómo	Generadores de Energía de Resguardo
Quién	Depto. Electricidad
Cuándo	Diciembre 2017
Recursos	Propios

Activo de Información	Registros de Gestión
Amenaza Identificada	Pérdida de información
Vulnerabilidad que podría explotar	Falta copia de resguardo
Valor Activo de Información	A
Accionar	
Mitigar	X
Transferir	
Aceptar	
Cómo	Acuerdo Nivel de Servicio
Quién	Depto. Centro de Cómputos
Cuándo	Diciembre 2017
Recursos	Propios

Activo de Información	RR.HH.
Amenaza Identificada	Divulgación de información
Vulnerabilidad que podría explotar	Falta Acuerdos de Confidencialidad
Valor Activo de Información	A
Accionar	
Mitigar	X
Transferir	
Aceptar	
Cómo	Acuerdos de Confidencialidad
Quién	Gerencia de RR.HH.
Cuándo	Diciembre de 2017
Recursos	Propios

Activo de Información	Lugar Físico
Amenaza Identificada	Deterioro Edilicio
Vulnerabilidad que podría explotar	Falta de mantenimiento
Valor Activo de Información	M
Accionar	
Mitigar	
Transferir	
Aceptar	X
Cómo	Acuerdo Nivel de Servicio
Quién	Depto. Servicios Generales
Cuándo	Diciembre 2017
Recursos	Propios

Activo de Información	Sistema de Aplicación
Amenaza Identificada	Caída del Sistema
Vulnerabilidad que podría explotar	Problema Hard/Soft
Valor Activo de Información	A
Accionar	
Mitigar	X
Transferir	
Aceptar	
Cómo	Acuerdo Nivel de Servicio
Quién	Depto. Análisis y Desarrollo / Depto. Tecnología
Cuándo	Diciembre 2017
Recursos	Propios

Activo de Información	Correo Corporativo
Amenaza Identificada	Código Malicioso
Vulnerabilidad que podría explotar	Día Zero del Código Malicioso
Valor Activo de Información	A
Accionar	
Mitigar	X
Transferir	
Aceptar	
Cómo	Buenas Prácticas Uso Correo Electrónico. Sistema Antivirus. Firma Digital.
Quién	Gerencia de Seguridad de la Información
Cuándo	Febrero 2018
Recursos	Propios

Activo de Información	Equipamiento Informático
Amenaza Identificada	Robo y fuga de información
Vulnerabilidad que podría explotar	Libre acceso a puertos usb y discos virtuales
Valor Activo de Información	A
Accionar	
Mitigar	X
Transferir	
Aceptar	
Cómo	Bloqueo de puertos usb. Bloqueo sitios con servidor proxy.
Quién	Depto. Tecnología / Depto. Telecomunicaciones
Cuándo	Diciembre de 2017
Recursos	Propios

Activo de Información	Información Digital
Amenaza Identificada	Pérdida de información
Vulnerabilidad que podría explotar	Falta copias de resguardo
Valor Activo de Información	A
Accionar	
Mitigar	X
Transferir	
Aceptar	
Cómo	Acuerdo de Nivel de Servicio
Quién	Depto. Centro de Cómputos
Cuándo	Diciembre de 2017
Recursos	Propios

Activo de Información	Información en Papel
Amenaza Identificada	Pérdida de información
Vulnerabilidad que podría explotar	Falta de Política Pantalla y Escritorios Limpios
Valor Activo de Información	A
Accionar	
Mitigar	X
Transferir	
Aceptar	
Cómo	Política de Pantallas y Escritorios Limpios
Quién	Gerencia de Seguridad de la Información
Cuándo	Diciembre de 2017
Recursos	Propios

Activo de Información	Instalación Eléctrica
Amenaza Identificada	Deterioro infraestructura cableado eléctrico
Vulnerabilidad que podría explotar	Falta mantenimiento
Valor Activo de Información	A
Accionar	
Mitigar	X
Transferir	
Aceptar	
Cómo	Acuerdo de Nivel de Servicio
Quién	Depto. Electricidad
Cuándo	Diciembre de 2017
Recursos	Propios

Activo de Información	Instalación de Datos
Amenaza Identificada	Deterioro infraestructura cableado de datos
Vulnerabilidad que podría explotar	Falta mantenimiento
Valor Activo de Información	A
Accionar	
Mitigar	X
Transferir	
Aceptar	
Cómo	Acuerdo de Nivel de Servicio
Quién	Depto. Telecomunicaciones
Cuándo	Diciembre 2017
Recursos	Propios

Activo de Información	Identidad Cliente
Amenaza Identificada	Robo de identidad
Vulnerabilidad que podría explotar	Falta de validación
Valor Activo de Información	A
Accionar	
Mitigar	X
Transferir	
Aceptar	
Cómo	PIN identificatorio e intransferible
Quién	Depto. Atención a Clientes
Cuándo	Diciembre de 2017
Recursos	Propios

Tabla 9: Gestión y Plan de Tratamiento del Riesgo

De esta manera tendremos efectuado un proceso de mitigación del riesgo mediante una metodología de trabajo. Los documentados utilizados, desde el punto de vista del formato, es opcional y ajustable a cada necesidad. Toda la documentación tiene que estar aprobada por la superioridad y debe ponerse en práctica. Como toda gestión se revisa, se identifican las correcciones y oportunidades de mejora y se actúa en consecuencia en cada caso. Esta metodología, al estar diseñada desde el punto de vista de seguridad de la información, es aplicable a toda la Organización.