DISEÑO DE UNA METODOLOGIA PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI, EN EL SECTOR DE LABORATORIOS DE ANALISIS MICROBIOLOGICOS, BASADO EN ISO 27001.

JOHANNA CAROLINA BUITRAGO ESTRADA

DIEGO HERNANDO BONILLA PINEDA

CAROL ESTEFANIE MURILLO VARON

UNIVERSIDAD EAN

FACULTAD DE POSTGRADOS

GERENCIAS DE PROCESOS Y CALIDAD

BOGOTÁ

2012

DISEÑO DE UNA METODOLOGIA PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI, EN EL SECTOR DE LABORATORIOS DE ANALISIS MICROBIOLOGICOS, BASADO EN ISO 27001.

INFORME FINAL DE INVESTIGACIÓN PRESENTADO COMO REQUISITO PARCIAL PARA OPTAR AL TÍTULO DE ESPECIALISTA EN GERENCIA PROCESOS Y CALIDAD.

FREDY REYES RONCANCIO
Ingeniero de Sistemas, Especialista en Administración de Empresas, Especialista en Gerencia de Tecnología, Magister en Ingeniería de Sistemas y Computación

UNIVERSIDAD EAN

FACULTAD DE POSTGRADOS

GERENCIAS DE PROCESOS Y CALIDAD

BOGOTÁ

2012

AGRADECIMIENTOS

Agradecemos a los docentes y la universidad EAN por la transferencia de conocimientos que nos permitió adaptar varias herramientas vistas durante la especialización de Gerencia de Procesos y Calidad, y proponerlas en esta guía metodología, herramientas que normalmente no son utilizadas en este contexto.

Al tutor Fredy Reyes por su acompañamiento y retroalimentación en el proceso de elaboración de esta guía.

Al grupo de trabajo por el aporte individual y colectivo que permitió consolidar los diferentes conocimientos propios de cada una de nuestras profesiones en este documento.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

1. RESUMEN

Los sistemas de información están expuestos cada vez a un mayor número de amenazas que constituyen un riesgo sobre uno de los activos más críticos y vulnerables de las organizaciones como la información. Asegurar la disponibilidad, la confidencialidad y la conservación de los datos, es un servicio que debe brindar la organización por lo que la gestión de la seguridad de la información debe realizarse mediante un proceso documentado y conocido. Este proyecto describe un diseño metodológico para la implementación de un sistema de seguridad de la información SGSI en el sector de laboratorios de análisis microbiológicos que garantice el nivel de seguridad y permita obtener la certificación ISO/IEC 27001:2005; se adopta como referencia las normas ISO 27001 y 27002. Finalmente, se concluye que la seguridad es un proceso de implantación que exige un cambio cultural y organizativo en las empresas.

ABSTRACT: The information systems are exposed every time to a major number of threats that constitute a risk on one of the most critical and vulnerable assets of the organizations, the information. To assure the availability, the confidentiality and the conservation of the information, it is a service that the organization must offer, It is why the management of the safety of the information must be realized by a documented and known process. This project describes a methodological design for the implementation of a safety system of the information SGSI in microbiological analyses laboratory, which guarantees the safety level and allows to obtain the certification ISO/IEC 27001:2005; it is adopted like it indexes the ISO procedure 27001 and 27002. Finally, one concludes that the safety is a process of implantation that demands a cultural and organizational change in the companies.

2. INTRODUCCIÓN

Los sistemas de información de las organizaciones desarrollan su misión en un entorno hostil. Las organizaciones son responsables de la protección de la información que gestionan ante las amenazas de este entorno y deben, por todos los medios disponibles, garantizar su confidencialidad, integridad y disponibilidad.

Desde hace tiempo, se percibe una creciente preocupación por todos los aspectos relacionados con la seguridad. Todas las organizaciones, públicas o privadas, grandes o pequeñas, se enfrentan día a día a amenazas contra sus recursos informáticos, con elevado riesgo de sufrir incidentes de alto impacto en su actividad. El imparable avance de las nuevas tecnologías en las organizaciones y, en general, el desarrollo de la Era de la información agrava constantemente esta situación.

Los riesgos que surgen relacionados con tecnologías y procesos, requieren soluciones y servicios emergentes. Soluciones para garantizar, de forma continua en el tiempo, la actividad de las organizaciones, la seguridad de la información base del negocio y los derechos de los individuos, en una sociedad cada vez más informatizada.

La seguridad no es un producto: es un proceso continuo que debe ser controlado, gestionado y monitorizado. Con el objetivo de ilustrar el contenido de la metodología, se analizará a lo largo de los diferentes capítulos el sector de laboratorios de análisis microbiológicos que se planteen abordar una estrategia de seguridad de la información para proteger sus datos e información tomando como base fundamental el modelo de mejora continua PHVA fundamentado en la norma ISO/IEC 27001. Primeramente se realiza la descripción del SGSI con la definición del escenario y la planeación (PLANEAR), el desarrollo del modelo desde su implementación hasta la gestión de la ejecución donde se fijan los controles y su aplicabilidad (HACER), después de que el SGSI se encuentra en marcha, se inician las actividades de monitorización y revisión (VERIFICAR) y finalmente se identifican las mejoras que se van hacer en el sistema (ACTUAR).

3. JUSTIFICACIÓN

Es de gran importancia la información manejada por los laboratorios de análisis microbiológicos como: las instalaciones, personal científico, la información de los clientes, procesos productivos, las muestras analizadas, los análisis basados en técnicas nacionales e internacionales y resultados reportados, los cuales son el objetivo principal de los servicios prestados por este sector y lo que provee sus beneficios económicos. Por lo tanto la seguridad de la información es responsabilidad de la organización al ser el apoyo de las industrias en el control de calidad de sus procesos y productos, planteando como objetivo asegurar resultados confiables a los clientes, cumpliendo además los requisitos del sistema de gestión de calidad basado en la ISO 17025/2005 (Requisitos generales para la competencia de laboratorios de ensayo y calibración).

De acuerdo con lo anterior es necesario diseñar una metodología para la implementación de un sistema de gestión de la seguridad de la información –SGSI-, teniendo como referencia la familia de las normas ISO 27000, para garantizar su disponibilidad, integridad y confidencialidad.

Este sistema permite identificar, gestionar y minimizar los riesgos reales y potenciales de la seguridad de la información por la organización, de una forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

4. OBJETIVOS

OBJETIVO GENERAL

Diseñar una metodología de implementación del sistema de gestión de seguridad de la información para empresas del sector de laboratorios de análisis microbiológicos de control de calidad, basado en la ISO 27001.

OBJETIVOS ESPECIFICOS

- Hacer de este documento una guía práctica para el lector en la que se expliquen los lineamientos de las normas que enmarcan la seguridad de la información, aclarando los requisitos y contextualizándolos en el sector de laboratorios de análisis microbiológico.
- Diseñar una metodología para la implementación y mantenimiento de la norma ISO27001 que involucre fase de planificación, implementación, revisión, mantenimiento y mejora.
- Proponer herramientas que faciliten la implementación de la norma IS0 27001 en cada una de sus etapas.

5. MARCO TEÓRICO

Actualmente nos encontramos en la era de la información y el conocimiento, las organizaciones deben tener como uno de sus principales objetivos el cuidado, seguridad y disponibilidad de sus activos de información; sin la adecuada preservación de la información de una empresa, esta perderá aquellas ventajas que la hacen ser competitiva y terminara por desaparecer del mercado; porque entre más tecnología y reconocimiento en las organizaciones mayor es el riesgo de la información si no existe protección contra amenazas y vulnerabilidades.

Para una adecuada gestión de la información es necesario implantar una ***metodología*** rigurosa y clara, que con base en ***normas*** preestablecidas le permitan a cualquier individuo de la organización asegurar la disponibilidad y seguridad de la información que maneja.

Para tener claros los conceptos a tratar en el marco teórico consulte el Anexo 1. Que contiene el glosario de los términos utilizados en este trabajo.

5.1 NORMAS ISO

La ***International Organization for Standardization*** - ISO e International Electrotechnical Commission – IEC, desarrollaron la familia de Normas ISO/IEC 27000, donde se proporcionan los lineamientos para la gestión de la seguridad en la información en cualquier empresa; para efectos de este trabajo nos enfocaremos en 3 de estas normas que mencionamos a continuación.

- **ISO 27001:** Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información y es a la cual se certifican por auditores externos los SGSI de las organizaciones. Este estándar

Internacional abarca todos los tipos de organizaciones, además específica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos comerciales generales de la organización. Específica los requerimientos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones individuales o partes de ella. EL SGSI está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas. [1]

- **ISO 27002:** Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. La norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005 (Ver Anexo 2.). Esta norma es la mejor práctica que da a los responsables los elementos necesarios para gestionar la seguridad de la información, las pautas para estructurar el plan y los objetivos de control, controles necesarios para implementar la seguridad y acciones fundamentales para minimizar los riesgos que la vulneren. [2]

- **ISO 27005:** Publicada el 4 de Junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Esta norma apoya el desarrollo de uno de los requisitos base para la implementación de la ISO 27001:2005 y el cumplimiento de otros como es la "valoración de los riesgos" que incluye la identificación, análisis, evaluación y tratamiento de los riesgos en la seguridad de la información. Adicionalmente brinda soporte y conceptos generales que se especifican en la 27001, y está diseñada con el

[1] ISO 27001:2005 Tecnología de la Información – Técnicas de seguridad – Sistemas de seguridad de la información - Requerimientos.
[2] Toro, M. 2011. Plan de seguridad de la información ISO 27002 Vs COBIT. Normas y Calidad. ICONTEC. Cuarta edición. P 26 – 28.

objetivo de facilitar la implementación de la seguridad de la información, con base en el enfoque de gestión de riesgo.[3]

5.2 SEGURIDAD DE LA INFORMACIÓN

La información representa valor para las organizaciones; por lo tanto es un activo ya que es un conjunto de datos, es esencial para el negocio de una organización, y en consecuencia es necesario asegurar su protección[4].

Como resultado del crecimiento tecnológico y la globalización, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades. La información puede existir en muchas formas: puede estar impresa o escrita en un papel, almacenada en magnético, enviada por correo o utilizando medios electrónicos, videos o grabaciones de voz. Sin importar la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debe estar protegida[4].

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

Revisando en términos generales la información que se puede manejar en un laboratorio u organización las amenazas se pueden clasificar en tres grupos:

- Externas: Intrusión a las redes de la organización o instalaciones físicas, por ejemplo: spam, hackers, suplantación de identidad, fraude, espionaje, sabotaje, robo de información, entre otras.

- Internas: Generadas al interior de la organización, principalmente por el conocimiento de los colaboradores. Ejemplo: Alteración de la información, divulgación de la información, fraudes, robo, sabotaje, uso no autorizados de sistemas informáticos, uso de imagen corporativa sin autorización, etc.

[3] Moreno, F. 2009. La ISO/IEC 27005 en la búsqueda de información más segura. Normas y Calidad. ICONTEC. Cuarta edición. P 28 – 32.

- Naturales: son generadas por desastres naturales, como inundaciones, huracanes, terremotos, incendios, etc.

Como lo resalta la ISO 27002:2005: La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio.

5.2.1 NECESIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

Establecer, documentar, implementar y mantener el Sistema de Gestión de Seguridad de la Información es importante para las organizaciones al representar una ventaja competitiva, flujo de caja, productividad, rentabilidad, estatus en el mercado y cumplimiento legal; al asegurar que la información, los procesos, la imagen corporativa y sistemas de apoyo son activos comerciales importantes.

Los activos de información de las organizaciones enfrentan amenazas de seguridad entre ellas: fraude por internet, computador, espionaje, sabotaje, hurto, fenómenos naturales, fuego o inundación. Las causas de daño como código malicioso, spam o hackers se hacen cada vez más comunes, más efectivas, más ambiciosas y cada vez más sofisticadas. De acuerdo a esto, la seguridad de la información es importante para todas las unidades de negocio sin importar que pertenezcan al sector público o privado.

En el mercado existe una variedad de software diseñados para ser seguros, aunque continúan presentándose amenazas y vulnerabilidades en la información, por esto es importante un trabajo integrado con la gestión y procedimientos adecuados, que permitan identificar qué controles son necesarios, lo cual se alcanza con la planeación, hacer, verificar y actuar del SGSI. La gestión de la seguridad de la información requiere, como mínimo, la participación de

todos los grupos de interés de la organización. Además es conveniente requerir asesoría especializada de organizaciones externas. [4]

Según la norma ISO 27002 de 2005 es esencial que una organización identifique sus requerimientos de seguridad. Existen tres fuentes principales de requerimientos de seguridad:

Una fuente se deriva de evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos de la organización. A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial.

Otra fuente son los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio; y su ambiente socio-cultural.

Otra fuente es el conjunto particular de principios, objetivos y requerimientos comerciales para el procesamiento de la información que una organización ha desarrollado para sostener sus operaciones.

5.3 PROCESOS PARA EL SECTOR DE LABORATORIOS DE ANÁLISIS MICROBIOLÓGICOS

Los laboratorios de análisis microbiológicos tienen como finalidad prestar un servicio para garantizar la calidad de los productos y procesos industriales en el área farmacéutica, cosmética, alimentos de consumo humano y veterinario, a través de controles específicos regulados por la secretaria distrital de salud y la Organismo Nacional de Acreditación ONAC en el caso que el laboratorio se encuentre acreditado bajo la norma ISO 17025: 2005.

[4] NTC-ISO/IEC 27002, Tecnología de la información. Código de práctica para la gestión de la seguridad de la información. Pag 10-11

5.3.1 MAPA DE PROCESOS Y CADENA DE VALOR

Para contextualizar los procesos del sector diseñamos el mapa de procesos y la cadena de valor para articular la metodología desarrollada.

En el mapa de procesos se identifica la entrada y la salida como las necesidades básicas, esperadas y expectativas del cliente, considerando los grupos de interés; en medio de las entradas y salidas se ubican los procesos misionales como punto central ya que están ligados al servicio que se presta y son percibidos directamente por el cliente; en la parte superior se encuentran los procesos de dirección como soporte para la toma de decisiones y como definición de la operación de la organización; finalmente los procesos de apoyo, en la parte inferior, determinantes para cumplir los objetivos de los procesos siendo el soporte en los procesos claves.

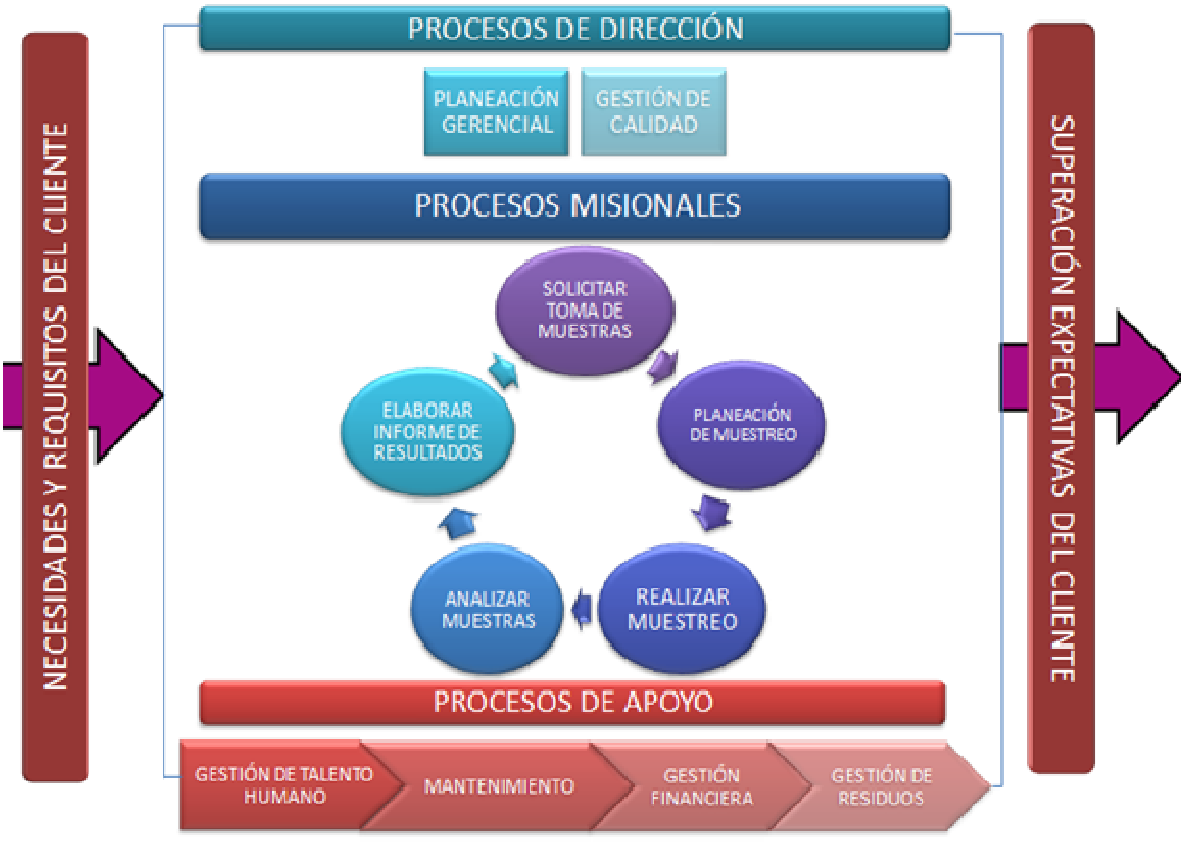


Ilustración 1 Mapa de Procesos Laboratorio de análisis microbiológico. Fuente: Los autores

La cadena de valor a continuación identifica las actividades que generan un valor enfocado al cliente, todos los aspectos que conforman la cadena junto con el mapa de procesos serán la guía para empalmar la metodología junto con el proceso genérico del sector.

Ilustración 2 Cadena de valor Laboratorio de análisis microbiológico. Fuente: Los autores

5.3.2 DESCRIPCIÓN DE LOS PROCESOS EN LABORATORIOS DE ANÁLISIS MICROBIOLÓGICOS

5.3.2.1 PROCESOS DE DIRECCIÓN

- **PLANEACIÓN GERENCIAL**

El objetivo de este proceso es definir el Sistema de Gestión Corporativo, su implementación y seguimiento, basado en estrategias que garanticen el control del día a día, la generación de proyectos y el mejoramiento del desempeño, a fin de alcanzar la visión propuesta del Laboratorio.

El sistema de Gestión Corporativo contempla los requisitos del cliente, identificando nuevas necesidades, de igual forma, determina los requisitos legales e internos del Laboratorio teniendo en cuenta las políticas corporativas. De acuerdo con las expectativas de la alta dirección de la compañía, su entorno y la necesidad de cumplir los requisitos del cliente y legales, se define el Plan Estratégico, la Política y los Objetivos de Calidad, los cuales deben ser coherentes entre sí e incluir la mejora continua del sistema.

Este proceso es importante integrar elementos de inteligencia corporativa –IC-, como un mecanismo que un equipo interdisciplinario en la organización tenga la capacidad de reunir, analizar y entregar oportunamente información relevante sobre el ambiente externo y las condiciones internas de una organización, para la toma de decisiones operativas y la orientación estratégica. Por lo tanto, la inteligencia corporativa incluye una visión global de los aspectos económicos, financieros, históricos, tecnológicos, sociales y regulatorios relacionados con la esfera de acción de la organización.

En el servicio de IC se debe considerar la realización de auditorías de información, para identificar el acceso y localización de fuentes de información, la tecnología disponible, la efectividad del flujo informativo o los canales de comunicación. Además el equipo de IC debe generar productos claros, concisos, completos, concretos y oportunos. La distribución establece la forma y la periodicidad de entrega del producto a través de informes impresos,

posters, boletines, audiovisuales, correo electrónico, presentaciones formales, conversaciones y reuniones, etc.[5]

- **GESTIÓN DE CALIDAD**

El objetivo del proceso de Gestión de Calidad es establecer, documentar, implementar y mantener un sistema de gestión para el laboratorio que cumple con las necesidades de sus clientes y mejora la gestión de la compañía, generando una sinergia entre los procesos. El sistema de gestión que aplica para los laboratorios de ensayo se basa la norma internacional ISO/IEC 17025:2005 y con los principios de ISO 9001:2000.

5.3.2.2 PROCESOS MISIONALES

El objetivo de estos procesos es asegurar la confiabilidad y trazabilidad de los análisis de Laboratorio y por tanto controlar los factores que lo determinan: Personal, instalaciones, condiciones ambientales, métodos de análisis, equipos, trazabilidad de la medición, muestreo y manejo de elementos de análisis.

Este proceso debe buscar incrementar el nivel de confianza de los clientes mediante el conocimiento y atención de sus necesidades y la prestación de un servicio de manera oportuna y eficiente. De esta manera asegurar las políticas y procedimientos que aumenten la competencia, imparcialidad, ética e integridad operativa.

Los procesos misionales son:

- **SOLICITAR TOMA DE MUESTRAS**

El cliente debe entregar una carta de remisión, E-mail o llamada que especifique todas las condiciones del muestreo: lugar, fecha, muestras a tomar, requisitos, objetivo. En el caso de que sea un contrato anual o mensual se establecerá previamente con el cliente un cronograma de muestreos donde se incluirá toda la información.

[5] Orozco, E. 1995. La Inteligencia Corporativa herramienta gerencial en la lucha por la competitividad. Transferencia de Tecnología. Publicación bimensual de la Fundación Tecnológica y del Instituto Tecnológico de Costa Rica. Noviembre – Diciembre 3 (15) .1

- **PLANEACIÓN DE MUESTREOS**

Una vez se recibe la información de las diferentes solicitudes de muestreo, se organiza el cronograma de acuerdo a los siguientes aspectos:

- Fechas exactas solicitadas por el cliente.
- Ubicación de las empresas a visitar.
- Asignación del responsable para la realización del muestreo.

- **REALIZAR MUESTREO**

La realización del muestreo en el punto que determine el cliente, se hace con base en el Procedimiento de Toma de muestras. En campo se diligenciará el registro de muestreo, en el cual se incluye la información de las características de las muestras recolectadas y demás información requerida. Es importante tener en cuenta el transporte de muestras, las cuales deberán ser transportadas y almacenadas según el Procedimiento establecido.

Este proceso incluye la recepción de muestras al laboratorio, donde se identifican con un código de acuerdo a lo establecido en el sistema de trazabilidad del laboratorio y se almacenan según la naturaleza de cada muestra a temperatura ambiente, refrigeración o congelación.

- **ANALIZAR MUESTRAS**

El procesamiento de las muestras inicia con la elaboración del plan de análisis de acuerdo a la normatividad que aplique o a los requisitos del cliente, teniendo en cuenta la naturaleza de la muestra. Posteriormente se continúa con la ejecución del plan de análisis, las muestras serán analizadas de acuerdo a los Procedimientos Operativos que corresponda según lo dispuesto en el plan de análisis. Durante el procesamiento de las muestras, se deberán llevar a cabo los controles que garanticen la calidad del procesamiento así como la confiabilidad de los resultados.

- **ELABORAR EL INFORME DE RESULTADOS**

Se compararán los resultados obtenidos con los límites permitidos, de conformidad con la naturaleza de la muestra, emitiendo el concepto respectivo sea ACEPTABLE O NO ACEPTABLE, cuando corresponda y apliquen límites establecidos por normatividad vigente o requisitos del cliente. Además se describe de forma detallada el resultado obtenido en los análisis efectuados teniendo en cuenta el concepto, microorganismos presentados y experiencia técnica.

El informe de resultados deberá además incluir: Codificación del informe, el nombre y dirección del laboratorio, paginación en cada página, nombre, dirección, teléfono y persona contacto del cliente, identificación de la muestra: Nombre, lote, cantidad, fecha producción, vencimiento, empaque, temperatura; Identificación del análisis: Fecha de recepción, fecha de proceso, identificación método y técnica utilizado, No de muestra, el protocolo de muestreo utilizado, los resultados obtenidos con unidad de medida y limite si lo requiere, el nombre y forma de quien lo Reviso y Aprobó, finalmente declaración de que el análisis es sólo valido para la muestra analizada.

En esta etapa de la emisión del informe de resultados generalmente se realiza una asesoría a los clientes que lo solicitan, para tomar acciones correctivas en los procesos y evaluar las causas de no conformidad.

5.3.2.3 PROCESOS DE APOYO

- **GESTIÓN DEL TALENTO HUMANO**

El objetivo de este proceso es asegurar el establecimiento de los parámetros necesarios para lograr un talento humano competente y comprometido con los objetivos corporativos. Se deben definir los cargos críticos y perfiles del Laboratorio, para establecer los criterios del proceso de selección de personal, realizar evaluaciones de competencia, ejecutar capacitaciones o actividades de formación y su respectiva evaluación.

1. Definir cargos críticos y perfiles: generalmente la organización puede establecer como cargos críticos todos los involucrados en el área comercial, administrativa y operativa. Se definen los perfiles de los cargos teniendo en cuenta el concepto de competencia: educación, experiencia, habilidades y formación.

2. Selección de personal: Esta etapa se desarrolla con base en los principios expuestos en el Procedimiento de Selección y Contratación de Personal establecido por el laboratorio. En éste, se relacionan los pasos a seguir en esta fase del proceso, así como las características del mismo.

3. Evaluación de la competencia del personal: Teniendo en cuenta los perfiles de cada cargo se establece la evaluación de la competencia del personal, que busca comparar el perfil del cargo contra las características de la competencia de quien lo ocupa.

   Del resultado de ésta evaluación, se determinará si la persona requiere algún tipo de formación o capacitación adicional, de ser necesario, se incluirá dentro del cronograma de capacitaciones.

4. Desarrollo de Capacitaciones o actividades de formación: es fundamental que todo su personal tenga claridad en los conceptos e información actualizada con respecto a microbiología, para que así sus actividades contribuyan al logro de los objetivos de la empresa. Para tal fin, realiza un adecuado proceso de inducción, reinducción y se generan capacitaciones en temas específicos para cada área. Las capacitaciones pueden ser internas o externas dependiendo de la necesidad. Así mismo y con el fin de minimizar la brecha entre las habilidades requeridas para el cargo y las habilidades del colaborador, se establecen programas de formación en habilidades administrativas, de desarrollo grupal, de innovación, etc.

5. Evaluación de la eficacia de la capacitación: Una vez desarrollada la capacitación, se busca evidenciar la eficacia de la misma. Para ello, es necesario determinar métodos de evaluación que sean objetivos.

- **MANTENIMIENTO**

El objetivo de este proceso es asegurar el mantenimiento preventivo de los equipos, software e instalaciones del laboratorio, además de un plan de contingencia en caso de que se presente alguna falla en los mismos y que pueda llegar a retrasar o afectar de alguna manera los análisis realizados.

- **GESTIÓN FINANCIERA**

El objetivo de este proceso es gestionar el presupuesto para la compra y/o contratación de bienes y/o servicios requeridos en el normal funcionamiento del laboratorio. Este proceso involucra la definición de los productos y servicios requeridos por el laboratorio, definir los proveedores críticos, la selección de proveedores, establecer criterios de evaluación de proveedores, determinar requisitos de la compra, la ejecución de la compra y la verificación del producto.

- **GESTION DE RESIDUOS**

El objetivo de este proceso de apoyo es establecer un plan en el cual se especifique la selección en la fuente de los residuos generados en el Laboratorio, junto con su inactivación y disposición final. Esto para garantizar el adecuado manejo de los residuos, para de esta manera mitigar el impacto ambiental.

6. METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL SGSI, EN EL SECTOR DE LABORATORIOS DE ANÁLISIS MICROBIOLÓGICOS.

Una de las principales características que debe poseer un empresa que busque establecer un SGSI es un enfoque por procesos, la norma ISO 27001 promueve la adopción del ciclo (Planear – Hacer – Verificar – Actuar) PHVA, para la definición de los procesos relacionados en el SGSI, aunque no es parte del alcance de presente documento el establecer una metodología para las organizaciones de cómo adquirir un enfoque por procesos, se darán una recomendaciones generales que ayudaran el lector a definir los procesos que intervendrán en el SGSI.

Con el fin de establecer una metodología general para la implementación de lo establecido en la norma ISO27001 para el sector de laboratorios de análisis microbiológicos en Colombia, seguiremos la metodología PHVA en la que enmarcaremos cada una de las etapas para la implementación del SGSI.

DEFINICIÓN DEL CICLO PHVA

El ciclo PHVA (o PDCA en ingles) es una herramienta de la mejora continua, diseñada por el Dr. Walter Shewhart en 1.920 y presentada por Deming a partir del año 1950, la cual se basa en un ciclo de 4 pasos: Planificar (Plan), Hacer (Do), Verificar (Check) y Actuar (Act)[6].

Es común usar esta metodología en la implementación de un sistema de gestión, de tal manera que al aplicarla en la política y objetivos del sistema, así como la red de procesos, la probabilidad de éxito sea mayor. Puede aplicarse a todos los procesos la metodología conocida como "Planificar- Hacer-Verificar-Actuar" (PHVA). PHVA puede describirse brevemente como:

[6] Plantilla para aplicar el ciclo PHVA. Tomado de: http://www.negociosyemprendimiento.org/2010/08/plantilla-para-aplicar-el-ciclo-phva-de.html

-Planear: establecer los objetivos y los procesos necesarios para conseguir los resultados de acuerdo con los requisitos del cliente y las políticas de la organización.

-Hacer: implementar los procesos.

-Verificar: realizar el seguimiento y medición de los procesos y los productos y servicios respecto a las políticas, los objetivos y los requisitos para el producto o servicio e informar los resultados.

-Actuar: tomar acciones para el mejoramiento continuo del desempeño de los procesos.

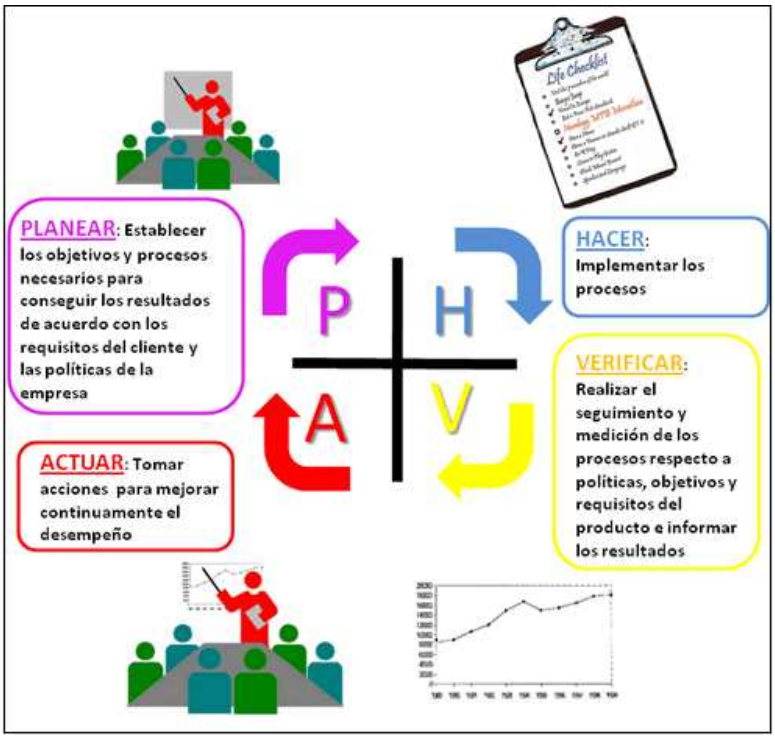


Ilustración 3 Ciclo PHVA Fuente: http://www.negociosyemprendimiento.org/2010/08/plantilla-para-aplicar-el-ciclo-phva-de.html

CICLO PHVA PARA EL SGSI

El diseño metodológico de este trabajo se basa en la metodología PHVA de la norma ISO 27001 para los SGSI, en la siguiente figura se pone en contexto la metodología propuesta en este documento dentro de cada etapa del ciclo.

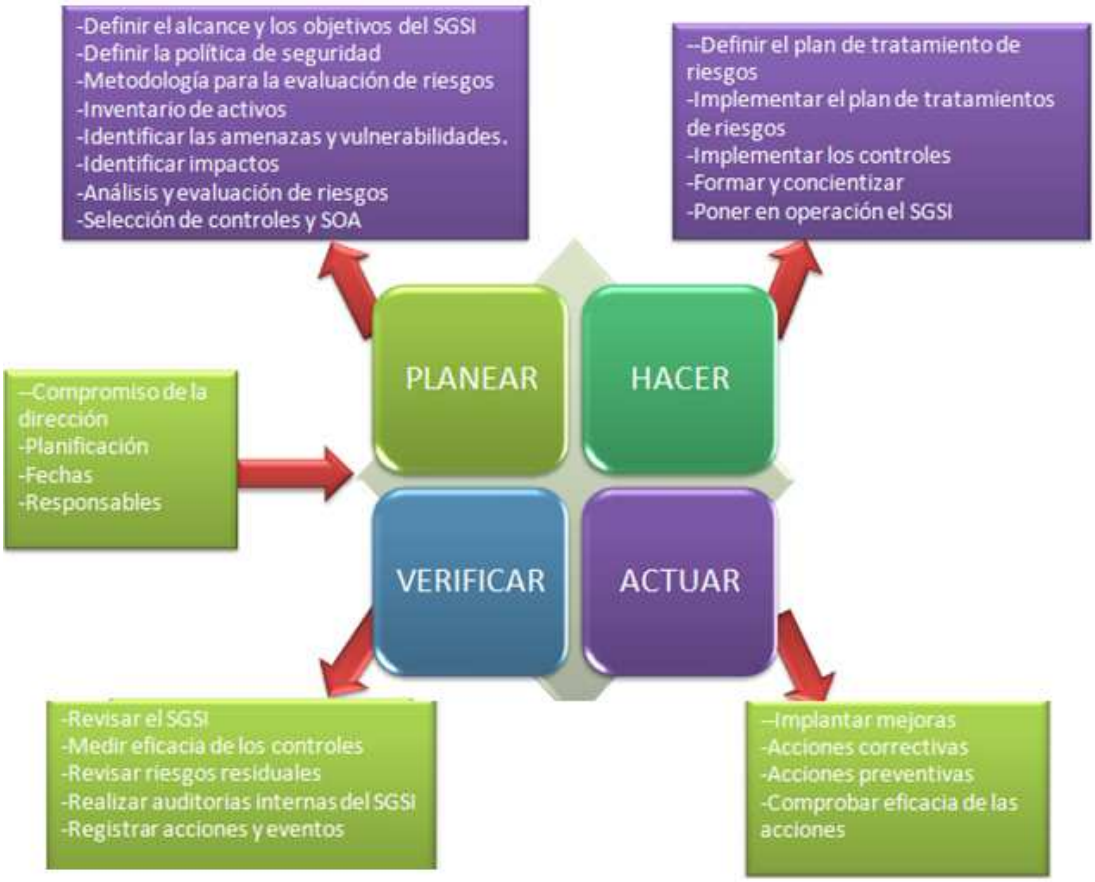


Ilustración 4 Ciclo PHVA para el SGSI. Fuente: http://www.iso27000.es/sgsi.html#section2d. Modificada por el autor.

En esta figura se encuentra un resumen general de la metodología propuesta, en el desarrollo de la misma se profundiza en cada entregable de las diferentes etapas del ciclo, ayudando al lector a desarrollar herramientas para cumplir los requisitos exigidos por la Norma ISO 27001.

En la siguiente tabla se relacionan los capítulos de las normas ISO 27001 e ISO 27002 en cada punto de la metodología planteada para ayudar al lector a mantener la correlación con la norma.

Tabla 1 Correlación de la metodología con las normas 27000. Fuente: El autor.

METODOLOGÍA	CAPÍTULO ISO 27001	CAPÍTULO ISO 27002
ARRANQUE DEL PROYECTO	5.1 y 5.2.1	
PLANEAR	4.2.1	
HACER	4.2.2. y 5.2.2.	5. a 15.
VERIFICAR	4.2.3., 6. y 7.	
ACTUAR	4.2.4. y 8.	
DOCUMENTACIÓN	4.3.	
DEFINICIONES	3.	

6.1 ARRANQUE DEL PROYECTO

El compromiso de la dirección es la base fundamental para iniciar el proyecto, el apoyo y la decisión de implementar el SGSI debe ser una decisión de la dirección de la organización. El cambio cultural que se debe vivir junto con la aplicación de la norma es un proceso que necesita del impulso constante de la dirección. La norma ISO 27001 establece los

compromisos que deben tener la dirección y la gestión de los recursos para lograr el funcionamiento del SGSI[7].

- Los compromisos de la dirección se deben evidenciar mediante el establecimiento de una política, objetivos y planes del SGSI; establecer funciones y responsabilidades de seguridad de la información; comunicar a la organización la importancia del cumplimiento de lo establecido; brindar los recursos necesarios; decidir criterios y niveles para aceptación de riesgo; asegurar que se realicen las auditorias internas y efectuar las revisiones del SGSI.

- La dirección debe provisionar los recursos necesarios para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI; asegurar que los procedimientos de seguridad de la información brindan apoyo a los requisitos del negocio; identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales; mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados; llevar a cabo revisiones cuando sea necesario y mejorar la eficacia del SGSI.

6.2 PLANEAR

En la etapa de planeación se define el alcance del sistema dentro de la organización y las políticas y lineamientos sobre los que se desarrollará, se presentan herramientas para la identificación, análisis y evaluación de riesgos, según el impacto de cada uno y el tipo de información que se afectaría, de igual forma es objetivo de esta etapa definir la forma de tratamiento de los riesgos identificados.

6.2.1 ALCANCE DEL SGSI

En primera medida la organización debe establecer el alcance del Sistema de Gestión de Seguridad en la Información SGSI, el alcance está en función de las características del negocio, la organización, localización, activos y tecnología por lo que definir el alcance no implica abarcar toda la organización, es más, es recomendable empezar por un alcance limitado, en el que se involucren los procesos *core* del negocio o que contengan la información más relevante para la compañía, es decir los que se han identificado en el mapa

[7] [4] IBID p 13.

como misionales. Es indispensable disponer del mapa de procesos, e identificar claramente aquellos que harán parte de alcance.

Tener claro las terceras partes y su influencia sobre la seguridad de la información, es importante en el momento de definir el alcance, los requisitos legales y contractuales relacionados con la seguridad de la información deben quedar contemplados también dentro del alcance del sistema.

Crear mapas de redes y sistemas, definir las ubicaciones físicas y disponer de organigramas organizativos facilita establecer con claridad el alcance del SGSI.

Para el caso de laboratorios de análisis microbiológico sugerimos que el alcance de SGSI se enfoque en los procesos misionales, típicamente definidos como

- Solicitar toma de muestras
- Planeación de muestreos
- Realizar muestreo
- Analizar muestras
- Elaborar informe de resultados

Cualquier otro proceso que la organización considere incluir dentro del SGSI es válido, lo que se recomienda es que la decisión de incluir más procesos sea con base en un análisis que en efecto sugiera la importancia de incluir dicho proceso, no se quiere hacer un SGSI muy robusto y poco efectivo, por el contrario, hacerlo lo más simple posible es una buena práctica, más aun cuando la organización empieza desde ceros el desarrollo del Sistema.

6.2.2 POLÍTICA DEL SGSI

Diferentes teorías de administración convergen en que una clara definición de la razón de ser de una organización normalmente denominada Misión, acompañado de un objetivo ambicioso, cuantificable y explicito para un periodo de tiempo, su Visión, es el pilar para poder desplegar las estrategias, procesos organizacionales y en general, para estructurar una empresa adecuada al cumplimiento de su propósito.

No es parte de los objetivos de este documento establecer los lineamientos para el desarrollo de la planeación estrategia, por el contrario, se supondrá que la organización tiene establecido dicho plan. En caso que no existiese, se recomienda establecerlo previamente; se sugiere consultar la norma ISO9001:2008 donde se encuentra valiosa información para este fin.

La política del SGSI entonces, debe estar alineada con los objetivos organizacionales, es allí donde la alta dirección debe establecer un marco de referencia para posteriormente fijar objetivos específicos de control por cada proceso de la compañía, los cuales deben establecerse en conjunto con el líder de cada proceso.

Ilustración 5 Política del SGSI. Fuente: Los autores.

La política del SGSI debe tener en cuenta el marco legal del laboratorio de análisis microbiológicos:

- ISO 17025:2005 Requisitos generales para la competencia de laboratorios de ensayo y calibración.
- Resolución 16078:1985 Requisitos de funcionamiento de laboratorios de control de calidad de alimentos.
- Decreto 2676: 2000 Gestión integral de residuos hospitalarios y similares.

- Decreto 4741: 2005 La prevención y el manejo de los residuos o desechos peligrosos generados en el marco de la gestión integral.
- Resolución 1164: 2002 Manual de procedimientos de gestión integral de residuos hospitalarios y peligrosos.
- Ley 1252: 2008 Referente a residuos peligrosos y material ambiental.

Parte fundamental en la implementación de sistema es la divulgación de la política trazada a toda la compañía con el fin de que las decisiones en los diferentes niveles de la compañía estén siempre alineadas con lo que la alta dirección espera del sistema, adicional, dejar clara la correlación o impacto de los objetivos genera mayor claridad de la razón de ser de los mismos y un mayor compromiso por parte de los responsables.

Finalmente la política debe contemplar los criterios y metodología para la valoración del riesgo, en donde se debe tener en cuenta lo siguiente:

- Determinar una metodología para la evaluación y clasificación de los riesgos que impactan la seguridad de la información.
- Identificar los riesgos
- Analizar y evaluar los riesgos encontrados
- Definir objetivos de Control y Controles para el tratamiento de riesgos
- Proponer opciones para el tratamiento de riesgos

La gestión de riesgo en la seguridad de la información, inicia al establecer el contexto, este se refiere a la definición del alcance, límites y la política del SGSI, con el fin de asegurar que todos los activos de información de la organización se contemplen en el SGSI. Es importante tener en consideración para los límites y criterios de aceptación de los riesgos: el tiempo, costo, recursos, impactos y requisitos legales para implementar los controles.

Al definir el contexto del SGSI, se realiza la valoración de los riesgos que involucra:

6.2.3 IDENTIFICACIÓN DEL RIESGO

La identificación del riesgo contempla inicialmente la determinación de los activos de información dentro del alcance del SGSI, teniendo en cuenta la ubicación, responsable y funciones. De igual manera se deben determinar las amenazas, vulnerabilidades e impactos en la organización, por las posibles pérdidas de confiabilidad, integridad y disponibilidad sobre los activos[3].

De acuerdo a lo anterior se realiza un inventario de activos relacionando cada proceso de la organización contemplado en el alcance del SGSI (Anexo 3), los activos hacen referencia a: personal de la organización, imagen corporativa, información, sistemas de información, procesos, productos, aplicaciones y el entorno físico.

A manera de ejemplo y para poner en contexto la aplicación de la metodología propuesta en el sector de laboratorios de análisis microbiológico, seleccionamos uno de los procesos misionales (Elaboración Informe de Resultados) para hacer el desarrollo de cada uno de los puntos.

Se estableció el Inventario de activos para el proceso de Elaboración de Informe de Resultados de acuerdo al formato diseñado en el anexo 3. En el numeral 6.2.5 se realiza la identificación del impacto para completar el formato.

ANEXO 3

LOGO DE LA ORGANIZACIÓN	INVENTARIO DE ACTIVOS DE INFORMACIÓN	CÓDIGO:	SGSI001	
		FECHA DE EMISIÓN	26/06/12	
		PAGINA	1 -1	

PROCESO	IDENTIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	PROPIETARIO/ RESPONSABLE	UBICACIÓN	C	I	A
Elaboración informe de resultados	Personal técnico	Usuarios	Director Técnico	Laboratorio			
	Instalaciones fisicas	Organización	Jefe de calidad	Coordenadas de la organización			
	Sistemas operativos/ plataforma	Software	Director Técnico	Servidor de la organización			
	Computadores	Hardware	Jefe de sistemas	Oficinas y laboratorio			
	Imagen corporativa	Organización	Director Técnico	Informe de resultados			
	Información del cliente	Información	Director Técnico	Base de datos / servidor de la organización			
	Información de las muestras	Información	Director Técnico	Libro de recepción de muestras / servidor de la organización			
	Datos del análisis	Información	Director Técnico	Servidor de la organización			
	Norma o referencia de limites permisibles	Información	Director Técnico	Servidor de la organización			
	Informe de resultados	Información	Director Técnico	Servidor de la organización			

C: Confiabilidad I: Integridad A: Disponibilidad

ELABORADO POR: Director Técnico APROBADO POR: Coordinador SGSI

Fuente: Los autores

Es importante tener claridad en los conceptos de amenaza y vulnerabilidad para identificarlas en el análisis de cada activo.

Amenaza: una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización[4]. Ejemplo: acceso no autorizado, código malicioso, spam, hackers, hurto por empleados o no empleados, mal uso de los sistemas de procesamiento

de la información, fraude, falla del sistema, negación del servicio, errores del usuario, desastres, etc.

Vulnerabilidad: la debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas[4]. Ejemplo: Falta de concientización, Falta de responsabilidades claras, Clasificación errónea de la información, Incapacidad de proporcionar evidencia, Falta de control de cambio o versión, Falta de mantenimiento, Identificación y autenticación inapropiada, Falta de seguridad de los medios, Falta de protección física, etc.

En el análisis de las amenazas y vulnerabilidades se requiere:

- ✓ Realizar una lista de las amenazas que puedan presentarse en forma accidental o intencional en la Empresa con relación a los activos de información. Diferenciar estas amenazas de las vulnerabilidades de los activos ya que el análisis debe radicar en las amenazas.
- ✓ Identificar los riesgos internos de los procesos analizando tanto las actividades que se desarrollan como las amenazas identificadas.
- ✓ Identificar los riesgos externos de los procesos. Es necesario analizar los riesgos que se pueden presentar cuando se subcontrata un servicio o existe personal externo a la organización.
- ✓ Realizar un análisis del entorno en los fenómenos naturales, el ambiente geopolítico, el ambiente tecnológico, el ambiente ecológico y los aspectos socioculturales que rodea la Organización para definir las amenazas a las que pueden estar expuestos los activos.

Ilustración 6 Amenazas y riesgos identificados en un laboratorio de análisis microbiológico. Fuente. Los autores

6.2.4 IDENTIFICACIÓN DEL IMPACTO

Una vez identificados los activos de información que posee la empresa para cada uno de los procesos que se han decidido incluir dentro del alcance del SGSI, se debe identificar cual sería el impacto que tendría en su respectivo proceso la pérdida o alteración de cada uno de los activos identificados.

Entiéndase impacto como el grado en el que se ve afectado determinado sistema, en este caso proceso, al alterar uno de sus componentes, para este caso activos de información. A mayor correlación entre el resultado del proceso y la alteración del activo, el impacto de ese activo será mayor.

Generalmente la evaluación del impacto viene de criterios subjetivos de los conocedores del proceso, en este documento se proponen 3 requisitos propios de los activos de información de una empresa, como lo describe la ISO 27001:2005 (Confidencialidad, Integridad y Disponibilidad), mediante los cuales se busca cuantificar el impacto que tiene dentro de su proceso. La definición de los 3 requisitos se encuentra en el anexo 1.

Para cada requisito se han establecido 3 niveles de impacto (bajo, mediano y alto) según se comporte el activo dentro del proceso, se recomienda que en el momento de decidir cuál de los 3 niveles aplica para cada categoría, se conforme un grupo interdisciplinar y se de un espacio abierto para la discusión, la cuantificación final debe salir de un acuerdo general del grupo, el ejercicio debe hacerse tomando activo por activo, evaluando los 3 requisitos antes de continuar con el siguiente.

A continuación se describen los requisitos para hacer de la identificación del impacto como un ejercicio objetivo:

Tabla 2 Requisitos de Confidencialidad. Fuente: Angelika Plate. ISO org.
http://es.scribd.com/doc/24326153/29/ISO-IEC-27005-Anexos-Anexos

REQUISITOS DE CONFIDENCIALIDAD (C)		
VALOR DEL ACTIVO	CLASE	DESCRIPCIÓN
1. BAJO	Disponible al público	La información no sensible y las instalaciones de procesamiento de la información y los recursos del sistema están disponibles para el público
2. MEDIANO	Para uso interno exclusivamente o uso restringido solamente	La información no sensible está restringida para uso interno exclusivamente, es decir, no está disponible para el público o la información restringida y las instalaciones de procesamiento de la información y los recursos del sistema están disponibles dentro de la organización con restricciones variadas con base en las necesidades de la empresa.
3. ALTO	Confidencial o estrictamente confidencial	La información sensible y las instalaciones de procesamiento de la información y los recursos del sistema están disponibles sólo sobre la base de la necesidad del conocimiento, o la información sensible y las instalaciones de procesamiento de información y los recursos del sistema están disponibles sólo sobre la base de la necesidad estricta del conocimiento.

Tabla 3 Requisitos de integridad. Fuente: Angelika Plate. ISO org.
http://es.scribd.com/doc/24326153/29/ISO-IEC-27005-Anexos.Anexos

REQUISITOS DE INTEGRIDAD (I)		
VALOR DEL ACTIVO	CLASE	DESCRIPCIÓN
1. BAJO	Baja integridad	El daño o modificación no autorizada no es crítico para las aplicaciones empresariales y el impacto en la empresa es insignificante o menor.
2. MEDIANO	Integridad mediana	El daño o modificación no autorizada no es crítico pero si es notorio para las aplicaciones empresariales y el impacto en la empresa es significativo.
3. ALTO	Integridad alta o muy alta	El daño o modificación no autorizada es crítica para las aplicaciones emresariales y el impacto en la empresa es importante y podría conllevar a la falta grave o total de la aplicación empresarial.

Tabla 4 Requisitos de Disponibilidad. Fuente: Angelika Plate. ISO org.
http://es.scribd.com/doc/24326153/29/ISO-IEC-27005-Anexos-Anexos

REQUISITOS DE DISPONIBILIDAD (A)		
VALOR DEL ACTIVO	CLASE	DESCRIPCIÓN
1. BAJO	Baja disponibilidad	Se puedes tolerar que el activo no este disponible por más de un día.
2. MEDIANO	Disponibilidad mediana	Se puede tolerar que el activo no esté disponible por máximo de medio día a un día.
3. ALTO	Alta disponibilidad	No se puede tolerar que el activo no esté disponible por más de unas cuantas horas, o incluso menos.

Es importante tener en cuenta los controles existentes en la organización para reducir los riesgos, ya que esto puede variar la valoración del impacto y las consecuencias sobre un activo de información[3]. Por ejemplo, se analizan las condiciones de instalaciones físicas de la organización, construcción, ubicación y alrededores, esto debe generar cierta seguridad que puede extenderse a los activos de información, y de esta manera la valoración del impacto es diferente.

Entre más acorde y aterrizado sea el análisis teniendo en cuenta la realidad actual de la organización más provechoso será el resultado de evaluación del impacto.

Para complementar el formato propuesto en el anexo 3 del inventario de activos, se realizó la identificación del impacto a los activos del proceso de elaboración de informe de resultados en el laboratorio de análisis microbiológico, evaluando los requisitos de confidencialidad, integridad y disponibilidad. Se realizó teniendo en cuenta condiciones normales de operación, en las cuales se realiza básicamente un backup de la información una vez a la semana, el personal ingresa al sistema del laboratorio con un usuario y una contraseña personal, los clientes tienen acceso a la web por medio de un usuario y contraseña para descargar los informes, todo el proceso se realiza en el software de manera trasversal y los datos de los resultados son disponibles para los analistas, quienes alimentan el sistema y el director técnico quien elabora el informe de resultados.

ANEXO 3

LOGO DE LA ORGANIZACIÓN	INVENTARIO DE ACTIVOS DE INFORMACIÓN	CÓDIGO:	SGSI001	
		FECHA DE EMISIÓN 26/06/12		
		PAGINA 1 -1		

PROCESO	IDENTIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	PROPIETARIO/ RESPONSABLE	UBICACIÓN	C	I	A
Elaboración informe de resultados	Personal técnico	Usuarios	Director Técnico	Laboratorio	Alto	Alto	Mediano
	Instalaciones fisicas	Organización	Jefe de calidad	Coordenadas de la organización	Mediano	Alto	Alto
	Sistemas operativos/ plataforma	Software	Director Técnico	Servidor de la organización	Alto	Alto	Alto
	Computadores	Hardware	Jefe de sistemas	Oficinas y laboratorio	Alto	Mediano	Alto
	Imagen corporativa	Organización	Director Técnico	Informe de resultados	Alto	Alto	Alto
	Información del cliente	Información	Director Técnico	Base de datos / servidor de la organización	Alto	Alto	Mediano
	Información de las muestras	Información	Director Técnico	Libro de recepción de muestras / servidor de la organización	Alto	Alto	Mediano
	Datos del análisis	Información	Director Técnico	Servidor de la organización	Alto	Alto	Alto
	Norma o referencia de limites permisibles	Información	Director Técnico	Servidor de la organización	Bajo	Mediano	Alto
	Informe de resultados	Información	Director Técnico	Servidor de la organización	Alto	Alto	Alto

C: Confiabilidad I: Integridad A: Disponibilidad

ELABORADO POR: Director Técnico APROBADO POR: Coordinador SGSI

Fuente: Los autores

6.2.5 ANÁLISIS Y EVALUACIÓN DEL RIESGO

La estimación del riesgo es el paso a seguir con el fin de valorarlo y determinar su importancia; puede ser cuantitativa al definir escalas de ocurrencia o cualitativa al usar escalas numéricas. El objetivo de esta etapa es obtener una lista de riesgos identificados de acuerdo a la probabilidad de ocurrencia de una amenaza y de sus consecuencias de los impactos, ligadas a las vulnerabilidades existentes a los activos de información. Por esta razón en la bibliografía se reporta que el riesgo en seguridad de la información se compone de tres elementos[3]:

Riesgo= activo de información + probabilidad + impacto

Para esta etapa se propone utilizar la matriz de Análisis Modal de Fallos y Efectos **AMFE**, de elementos clave de procesos o productos. Esta herramienta es una de las tradicionales empleadas en el ámbito de la Calidad para la identificación y análisis de potenciales desviaciones de funcionamiento o fallos. Se trata de un método cualitativo que por sus características, resulta de utilidad para identificar los puntos de fallo potenciales, y elaborar planes de acción para combatir los riesgos, y facilitar acciones en prevención de riesgos[8].

Como paso previo a la descripción del método y su aplicación es necesario sentar los términos y conceptos fundamentales, que a continuación se describen:

Detectabilidad:

Este concepto es esencial en el AMFE. Si durante el proceso se produce un fallo o cualquier "output" defectuoso, se trata de averiguar la probabilidad que no lo "detectemos", pasando a etapas posteriores en el proceso, generando los consiguientes problemas y llegando en último término a afectar al usuario final, en este caso al propietario del activo de información y si es el caso a toda la organización. Cuanto más difícil sea detectar el fallo existente y más se tarde en detectarlo más importantes pueden

[8] Bestratén, M. Orriols, R. Y Mata, C. Análisis modal de fallos y efectos AMFE. Instituto Nacional de Seguridad e Higiene en el trabajo. Notas Técnicas de Prevención. 679. P 1 - 8.

ser las consecuencias del mismo[8]; es decir el impacto del riesgo generado en el activo es mayor cuando no se detecta a tiempo. En la tabla 5 se indica la clasificación de la facilidad de detección del riesgo.

Tabla 5 Clasificación de la facilidad de detección del riesgo. Fuente. Los autores

DETECTABILIDAD	CRITERIO	VALOR
Muy alta	Detección obvia	1
Alta	Facilmente detectable con un control	2
Mediana	Detectable despues de varios controles	3
Minima	Dificil detección	4
Improbable	No puede detectarse	5

Frecuencia:

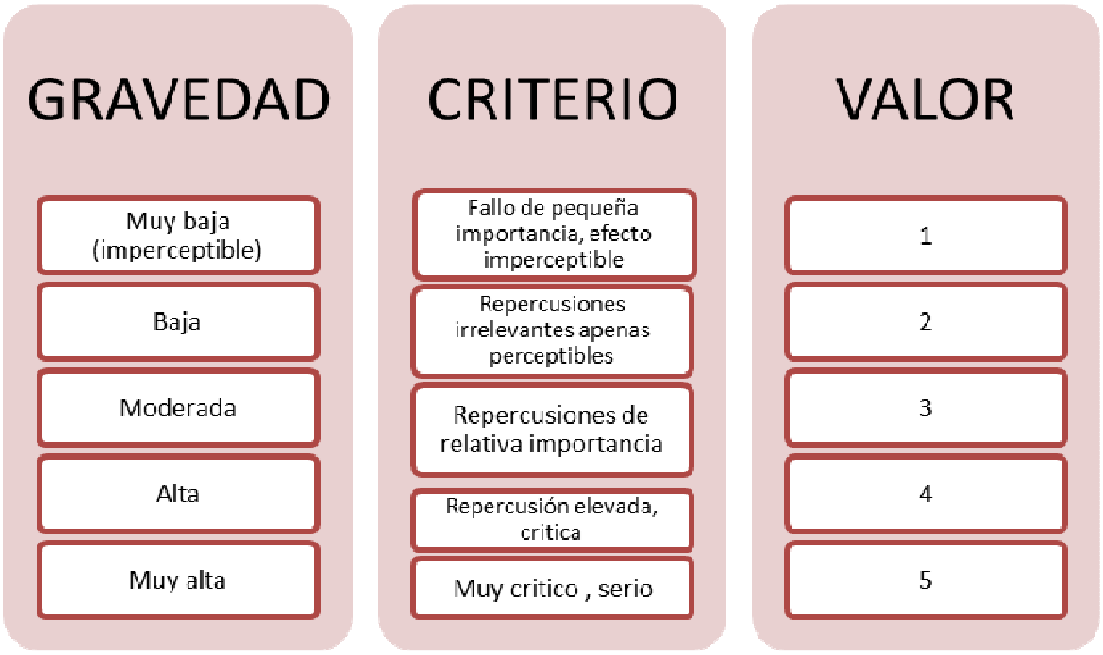
Mide la repetitividad potencial u ocurrencia de un determinado fallo, es lo que en términos de fiabilidad o de prevención llamamos la probabilidad de aparición del fallo[8].

Tabla 6 Clasificación de la frecuencia o probabilidad de ocurrencia. Fuente. Los autores

Gravedad:

Mide el daño normalmente esperado que provoca el fallo en cuestión, según la percepción del propietario del activo y del equipo del SGSI, para que no sea subjetivo el análisis. También cabe considerar el daño máximo esperado, el cual iría asociado también a su probabilidad de generación[8]. En la matriz AMFE se puede calificar de acuerdo a la escala de 1 a 5 como lo indica la tabla 7.

Tabla 7 Clasificación de la Gravedad del riesgo. Fuente. Los autores



Índice de Prioridad de Riesgo (IPR):

El índice de prioridad del AMFE incorpora el factor detectabilidad. Por tanto, tal índice es el producto de la frecuencia por la gravedad y por la detectabilidad, siendo tales factores traducibles a un código numérico adimensional que permite priorizar la urgencia de la intervención, así como el orden de las acciones de control o tratamiento en este caso de seguridad de la información. Por tanto debe ser calculado para todas las causas de fallo[8].

IPR = D.G.F

El IPR es el producto de los tres factores que lo determinan. Dado que tal índice va asociado a la prioridad de intervención, suele llamarse Índice de Prioridad del Riesgo. Debe ser calculado para todas las causas de fallo. No obstante un IPR inferior a 100 ó 50 según los límites del SGSI no requeriría intervención salvo que la mejora fuera fácil de introducir y contribuyera a mejorar aspectos de calidad del proceso. Es importante que la organización evalué y establezca en el contexto del SGSI los límites del IPR, para decidir en la matriz AMFE cuales riesgos necesitan tratamiento; porque el IPR ofrece una primera aproximación de la importancia del riesgo, lo que ha de facilitar la toma de decisiones para determinar el control o tratamiento del riesgo[8].

En la aplicación de la matriz AMFE en seguridad de la información (ver tabla 8), el termino fallo o modo de fallo hace referencia al riesgo potencial que es identificado en el proceso o en una actividad específica del mismo; ya que el objetivo es identificar los riesgos en todo el despliegue de los procesos. El concepto causa a modo de fallo, describe la amenaza, es decir lo que puede causar el daño o pérdida del activo por medio de la explotación de las vulnerabilidades del activo de información.

En el caso de la aplicación en un laboratorio de análisis microbiológicos, el análisis de riesgos se realiza por proceso definiendo cada una de las actividades y luego los activos de información de cada actividad, como se observa en la matriz AMFE para el proceso de elaboración de informes de resultados, en la cual se analiza cuáles son los riesgos, los efectos y las amenazas.

Tabla 8 Matriz AMFE para el SGSI.

Fuente. Los autores

MATRIZ AMFE

PROCESO: ELABORACIÓN DE INFORME DE RESULTADOS | **RESPONSABLE DEL ÁREA:** DIRECTOR TÉCNICO | **PARTICIPANTES DE LA ORGANIZACIÓN:** COORD. DE CALIDAD, DIRECTOR TÉCNICO, COORD. SGSI | **VERSIÓN:** 01 **FECHA DE ELABORACIÓN:** 26/06/12

ACTIVIDAD / OPERACIÓN	ACTIVO DE INFORMACIÓN	PROPIETARIO /RESPONSABLE	FALLO Nº	FALLOS POTENCIALES			ESTIMACIÓN				AREAS RELACIONADAS CON EL ACTIVO
				MODO DE FALLO	EFECTOS	CAUSAS DEL MODO DE FALLO	F	G	D	IPR	
Codificar el informe	Sistema operativo del laboratorio	Director técnico	1.1	Asignación de código equivocado	Error en el sistema de trazabilidad	Falla del servidor y del sistema. Falla en el registro de muestras.	2	3	2	**12**	Operativa y dirección técnica
			1.2	Mal funcionamiento del servidor	Perdida de tiempo. Error en la trazabilidad	Sobrecarga de energía. Falta de energía. Falla en la conectividad del sistema.	3	5	1	**15**	
Comparación de resultados Vs limites permitidos	Personal técnico		2.1	Ajuste de resultados por conveniencia	Resultados no confiables.	Alteración de los resultados. Falta de responsabilidad del DT.	1	5	4	**20**	
	Datos de análisis		2.2	Perdida de confidencialidad	Rompimiento contractual con el cliente. Se genera mala imagen del cliente y del laboratorio. Quejas.	Divulgación de la información.	2	5	3	**30**	
			2.3	Perdida de información	Reproceso de análisis. Retraso en la entrega de resultados. Quejas del cliente.	Robo de información. Sabotaje. Espionaje. Acceso no autorizado al software del laboratorio	2	5	2	**20**	
	Norma o referencia de limites permisibles		2.4	Incoherencia en la comparación de los resultados	Error en la emisión del informe. Quejas del cliente.	Uso de normatividad que no aplica. Falta de capacitación.	2	4	2	**16**	
Definir el concepto (aceptable o no aceptable)	Personal técnico		3.1	Dar un concepto errado al resultado de la muestra	Reproceso de análisis. Queja del cliente. Desconfianza al cliente.	Falta de capacitación. Falta de tiempo para la revisión.	2	5	2	**20**	
Verificar información del cliente	Información del cliente		4.1	Asignar el cliente equivocado	Queja del cliente. Problemas de confidencialidad. Error en la trazabilidad	Falla del servidor y del sistema. Falla en el registro de muestras. Falta de tiempo para la revisión.	1	4	2	**8**	
Verificar información de la muestra	Información de las muestras		5.1	Asignar la información equivocada de la muestra (lote, fechas, etc)	Queja del cliente. Problemas de confidencialidad. Error en la trazabilidad	Falla del servidor y del sistema. Falla en el registro de muestras. Falta de tiempo para la revisión.	2	4	2	**16**	
Envio o entrega del informe	E-mail del cliente / contacto para entrega		6.1	Envio del informe al correo equivocado	Rompimiento de confidencialidad. Queja del cliente.	No verificación del e-mail. Falta de conocimiento de la información.	2	5	2	**20**	
	Informe de resultados		6.2	Plagio del informe de resultados	Resultados no validos.	Acceso no autorizado al software del laboratorio. Sabotaje. Fraude.	1	5	3	**15**	
			6.3	Emisión de informes de resultados no confiables por conveniencia.	Problemas de salud pública. Quejas.	Alteración de los resultados. Falta de revisión de los resultados preliminares. No alertar al cliente a tiempo.	1	5	3	**15**	
			6.4	Perdida de información	Reproceso. Aumento de costos. Retraso en la entrega del informe.	información. Sabotaje. Espionaje. Acceso no autorizado al software del laboratorio. Desorden en el almacenamiento de los informes.	3	4	2	**24**	
	Sistema operativo del laboratorio		6.5	Perdida de información por fallos en el servidor	Reproceso. Aumento de costos. Retraso en la entrega del informe.	Virus. Código malicioso. Hackers. Espionaje. Robo	2	5	3	**30**	
	Computadores		6.6	Perdida de información del PC	Problemas de trazabilidad. Retraso del proceso.	Virus. Código malicioso. Hackers. Espionaje. Robo. Acceso no autorizado.	3	4	1	**12**	
	Imagen corporativa		6.7	Perdida de estatus y reconocimiento del laboratorio en el mercado	Mala imagen del laboratorio. Rompimientos contractuales con los clientes.	Uso indebido de la imagen corporativa. Suplantación de identidad. Sabotaje. Fraude.	1	5	4	**20**	
	Instalaciones fisicas		6.8	Incumplimiento en la entrega del informe de resultados.	Quejas. Reprocesos. Aumento de costos.	Falta de energía. Inundación. No disponibilidad de los equipos.	2	4	1	**8**	Calidad

F: Frecuencia
G: Gravedad
D: Detectabilidad
IPR: Indice de prioridad del riesgo

APROBADO POR: Gerente general

La evaluación del riesgo se realiza a partir de los límites y criterios definidos en el contexto del SGSI, el objetivo es comparar el resultado de la estimación del riesgo con los criterios y aceptación definidos. En esta etapa se define la prioridad de los riesgos que deben ser tratados y gestionados, de acuerdo al resultado de la matriz AMFE y al analizar el índice de prioridad del riesgo IPR.

En el análisis de riesgos del proceso de "elaboración de informes de resultados", la matriz AMFE permite evaluar la frecuencia, gravedad y detectabilidad de cada riesgo identificado. En este caso aplicado es conveniente dar prioridad a los IPR de 15 o superior, es importante aclarar que este criterio lo debe definir la organización en las políticas del SGSI. Los riesgos con un IPR de 15 o mayor presentan una gravedad alta que perjudica a la organización y a la calidad del proceso. Por esta razón es conveniente este criterio de IPR. Por ejemplo el plagio de informes de resultados, la perdida de información por fallos en el servidor y la perdida de confidencialidad son riesgos que pueden afectar el estatus del laboratorio, el rompimiento contractual con los clientes, el incumplimiento en la entrega de resultados, aumento de costos por reproceso, lo cual se despliega en la calidad de los procesos y servicios de la organización, con un efecto considerable en la rentabilidad.

6.3 HACER

Siguiendo la metodología del PHVA, trataremos en este punto el desarrollo del paso HACER, inicialmente se debe definir el plan de tratamiento de los riesgos que se identificaron en el punto anterior, la manera de gestionar estos riesgos y la selección y aplicación de los controles para mitigarlos. Cuando se implemente el plan de tratamiento y los controles se debe alcanzar los objetivos de control que se identificaron en el planear. Para el desarrollo de este punto es necesario tomar como punto de referencia la norma ISO 27001:2005 la cual establece las directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en la organización. Como segundo paso se debe empezar con una toma de conciencia y formación de todo el personal de la organización en lo relativo a la seguridad de la información. Si este paso no se lleva acabo el SGSI no va tener ningún sentido y no va generar los beneficios de la implementación, para lograr esto sugerimos desarrollar el marco normativo necesario, las normas, los manuales, los procedimientos e instrucciones que

permitan gestionar las operaciones del SGSI y los recursos asignados además recomendamos implementar procedimientos y controles de detección y respuesta a incidentes de seguridad que van a evaluar la efectividad de los controles en funcionamiento. Teniendo en cuenta lo anterior el HACER contempla[9]:

- Definir el plan de tratamiento de riesgos
- Implementar el plan de tratamientos de riesgos
- Implementar los controles
- Formar y concientizar
- Poner en operación el SGSI.

6.3.1 PLAN DE TRATAMIENTO DEL RIESGO

La gestión de los riesgos es un proceso en el cual se implementan las medidas técnicas y organizativas necesarias para impedir, reducir o controlar los riesgos analizados e identificados, de forma que las consecuencias que puedan generar sean eliminadas o, si esto no es posible, se puedan reducir lo máximo posible. Un resultado del análisis de riesgos es el criterio para determinar los niveles de riesgo aceptables y en consecuencia, cuáles son los niveles inaceptables y que por lo tanto serán gestionados. El objetivo es reducir los riesgos que estén por encima de los niveles aceptables, a niveles que puedan ser asumidos por la organización[10].

[9] [4] IBIP p 13.

[10] Poveda, J. Gestión y tratamiento de los riesgos, 2007. http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-9.pdf.

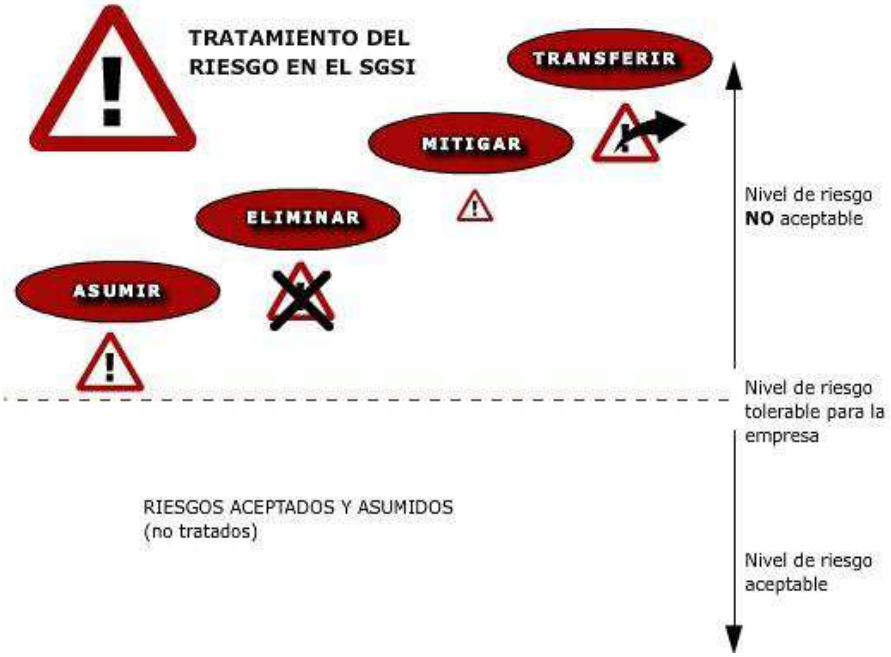


Ilustración 7 Tratamiento del riesgo en el SGSI. Fuente: Poveda, J. Gestión y tratamiento de los riesgos, 2007.

Una vez se han analizados y se conocen los riesgos de la organización se determinara el tratamiento que deben recibir los activos y se deben tomar las acciones necesarias. Los cuatro tipos de tratamiento requieren de diferentes acciones:

- **Mitigar el riesgo:** Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.

- **Asumir el riesgo:** La Dirección asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado que la dirección conoce y acepta estos riesgos. Los riesgos que se han asumido han de ser controlados y revisados periódicamente de cara a evitar que evolucionen y se conviertan en riesgos mayores.

- **Transferir el riesgo a un tercero:** Como por ejemplo, asegurando el activo que tiene el riesgo o subcontratando el servicio. Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y

del coste de realizar esta transferencia (no sólo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).

- **Eliminar el riesgo:** Aunque no suele ser la opción más viable, ya que puede resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo.

No habrá más acciones a la hora de gestionar los riesgos para la correcta implantación de un sistema de gestión de la seguridad de la información, ya que una organización que conoce sus riesgos jamás podrá ignorarlos, puesto que, de este modo, no estaría vigilando y daría lugar a un incidente de seguridad. Una vez decididas las acciones a tomar, se debe realizar un nuevo análisis de riesgos, teniendo en cuenta la nueva situación considerando que los controles y medidas que se ha decidido implantar van a reducir en mayor o menor medida el riesgo que existía, ya que ese es su objetivo. En una organización nunca se podrá eliminar totalmente el riesgo, siempre quedará un cierto nivel de riesgo, por lo que es importante que todos los riesgos residuales sean aceptados por la Dirección[11].

6.3.2 MITIGACIÓN DEL RIESGO

Una vez se han identificado los requisitos y los riesgos de seguridad y se han tomado las decisiones para el tratamiento de los riesgos, es conveniente seleccionar e implementar los controles para garantizar la reducción de los riesgos hasta un nivel aceptable. Los controles se pueden seleccionar a partir de la norma ISO 27002:2008 (ver Anexo2.) o diseñar controles nuevos para satisfacer necesidades específicas de la organización. La selección de los controles de seguridad depende de las decisiones del laboratorio basadas en los criterios para la aceptación del riesgo y debería estar sujeta a toda la legislación y los reglamentos.

PASOS PARA MITIGAR EL RIESGO:

- Seleccionar los controles apropiados para los riesgos que se han analizado y se determino tratar, en principio del Catálogo de Buenas Prácticas de la ISO/IEC 27002

[11] IBIP p 48.

(133 controles posibles), pero pueden añadirse otros que el laboratorio considere necesario.

- Diseñar los procedimientos para implantar los controles aunque sean controles técnicos es necesario procedimiento de instalación, uso y mantenimiento.
- Verificar que los controles estén correctamente implantados.
- Establecer indicadores que permitan medir la implementación de los controles y si reduce el riesgo al nivel de aceptación.

Ilustración 8 Tratamiento del riesgo en el SGSI. Fuente: Poveda, J. Gestión y tratamiento de los riesgos, 2007.

6.3.2.1 SELECCIÓN DE CONTROLES

Los controles se seleccionarán e implementarán para minimizar en lo posible la posibilidad de que los riesgos detectados en el análisis de riesgos dañen los activos. Existen dos grandes grupos de controles. Por un lado los técnicos, tales como sistemas de cifrado, copias de seguridad, sistemas de detección de intrusos, actualizaciones de software, antivirus o cortafuegos, y por otro los organizativos que son medidas organizativas tales como la Política de Seguridad, procedimientos de uso de los sistemas de información para los usuarios, los planes de formación o los planes de continuidad del negocio.

Es muy importante conseguir un conjunto de controles que contenga controles de los dos tipos, ya que muchas medidas técnicas no pueden impedir que los usuarios de los sistemas cometan errores o dañen intencionadamente los activos y, al contrario, emitir muchas normas internas puede ser inútil si no hay una mínima seguridad técnica implantada.

Otra clasificación que se puede hacer de los controles para facilitar su selección es la de controles preventivos y correctivos. Los controles de tipo preventivo son aquellos que sirven para evitar incidentes de seguridad no deseados mientras que los correctivos son aquellos que se pondrán en marcha ante la ocurrencia de fallos o incidentes de seguridad.[12]

Se deben tener en cuenta diferentes factores y restricciones en el momento de la selección de controles como son el costo de la implementación y mantenimiento del control, la disponibilidad, la ayuda que se debe brindar a los colaboradores para desempeñar el control y su aplicabilidad con respecto a los riesgos que se han detectado.

No todos los controles deben ser seleccionados, pero hay algunos que son requisito de la norma UNE/ISO-IEC 27001 tales como la Política de Seguridad o las auditorías internas.

6.3.2.2 IMPLEMENTACIÓN DE CONTROLES

Seleccionados los controles pertinentes, debe definirse los procedimientos para su implantación. Los controles de tipo organizativo se prestan más a ser implantados mediante procedimientos, como por ejemplo la gestión de los recursos humanos. Pero incluso los de corte tecnológico pueden ser susceptibles de necesitar documentación, como por ejemplo la realización de copias de seguridad. Debe analizarse la lista de controles seleccionados y establecer qué procedimientos necesitan ser desarrollados. Hay que contar también que si la organización no tiene procesos muy complejos puede ser posible que varios controles puedan agruparse en un único procedimiento. No es necesario ni recomendable, desarrollar un procedimiento para cada control. La cantidad de documentación generada puede hacer francamente difícil que se logren gestionar correctamente los controles. Por otro lado, los procedimientos deben ser lo más breves y claros posible. No deben incluir demasiadas instrucciones ni particularidades de la tarea a realizar. El objetivo del procedimiento es contar

[12] Guía de seguridad de la información para pymes. Región de Murcia. 2009.

con una herramienta que permita a cualquiera ejecutarla con un mínimo de rigor aun sin contar con formación o experiencia previa.

6.3.2.3 VERIFICACIÓN DE CONTROLES

Una vez puestos en marcha, debe comprobarse periódicamente que los controles funcionan como se esperaba. Si no es así, deberán tomarse las acciones necesarias para corregir esa situación. Una herramienta fundamental del SGSI es la verificación de la eficacia de los controles implantados. Para ello deben establecerse objetivos de rendimiento para los controles, marcar puntos de control y medición y registrar los resultados de manera que se sepa si el control realmente protege los activos hasta el punto que la organización necesita.

6.3.2.4 DOCUMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS

La documentación de la gestión de riesgos se realiza mediante la Declaración de Aplicabilidad también conocida por sus siglas en inglés SOA ("Statement Of Applicability"). Este documento, requerido por la Norma UNE/ISO-IEC 27001, es un resumen de las decisiones que se han tomado para tratar los riesgos analizados y debe incluir los 133 controles del Anexo A de la Norma, mas los controles adicionales a los de la Norma que la organización hubiera estimado conveniente aplicar. Para cada uno de los controles debe reflejarse en este documento[13]:

- Si está implantado actualmente en la organización, con una breve descripción de cómo se aplica.
- Si se va a implantar, es decir, si es uno de los controles escogidos para mitigar el riesgo, junto con las razones para haberlo seleccionado.
- Si no se va a implantar, y entonces hay que exponer los motivos que han llevado a esta decisión. Las exclusiones deben justificarse adecuadamente.

Este documento constituye de alguna manera un registro de los resultados finales del SGSI, ya que concreta de manera clara y directa en qué va a consistir el sistema de seguridad, detallando cada uno de los controles que se tiene la intención de aplicar de manera explícita.

[13] [4] IBIP p 13.

Sólo insistir en que no es necesario seleccionar todos los objetivos ni todos los controles asociados a cada uno de los objetivos. Deben escogerse los objetivos y controles apropiados a las circunstancias, es decir, aquellos que se considera que cubren los requisitos de seguridad de la organización y son viables. Una vez que está claro que se va a hacer, debe prepararse un plan para la realización de todo lo que se ha decidido hacer. Este plan, que la Norma denomina Plan de Tratamiento de Riesgos, contempla todo las acciones necesarias tanto para implantar el SGSI y gestionarlo como para la puesta en marcha de los controles escogidos. El plan tiene que contar con los recursos materiales, técnicos y humanos necesarios para que pueda ser llevado a cabo con ciertas garantías de éxito. Debe ser revisado a intervalos regulares para comprobar que no se producen desviaciones. Estas pueden ser de plazo porque no hay recursos para ejecutarlas o han resultado ser más difíciles de ejecutar de lo que se preveía en un principio o también de que no se llevan a cabo las acciones planificadas sino otras, normalmente porque se han tomado decisiones sobre la marcha para solventar problemas no previstos. Dentro de este plan pueden quedar recogidos los objetivos definidos para medir la eficacia de los controles, estableciendo asimismo el mecanismo de recogida y análisis[14].

6.3.3 CONTROLES E IMPLEMENTACIÓN PARA EL SECTOR DE LABORATORIOS DE ANÁLISIS MICROBIOLÓGICOS15

A continuación se relacionan las principales medidas de seguridad relacionadas directamente con el sector de laboratorios farmacéuticos, los controles y su implementación, tomando como base la norma ISO/IEC 2002:2008 (Ver Anexo 2. Y Anexo 3.).

[14] Carozo, E. Implantación de un sistema de gestión de seguridad de la información en una empresa compleja. Universidad de Montevideo. 2007.

[15] [4] IBID p 13.

6.3.3.1 CONTROLES Y OBJETIVOS DE CONTROL RELACIONADOS CON EL MARCO DEL LABORATORIO

En el marco de la seguridad de la información como estrategia para proteger los activos de información de la organización, esta debe contemplar los objetivos del negocio como un requisito imprescindible para la planificación de actuaciones. Para que las medidas adoptadas sean efectivas, la dirección debe adoptar y mantener un compromiso con los planes de seguridad de la organización. Entre las principales actuaciones que han de tener el respaldo directo de la dirección están: establecer una política de seguridad, definir directrices claras para el tratamiento de la información, promover una estructura de clasificación de la información, definir normas de etiquetado de soportes, establecer procedimientos que regulen las comunicaciones y relaciones con terceros y asegurar el cumplimiento de todos los aspectos legales que obliguen a la organización en materia de tratamiento de la información[16].

A. DEFINICIÓN DE LA POLÍTICA DE SEGURIDAD DE LA EMPRESA

Establecer una adecuada Política de Seguridad tiene un doble propósito, informar y concientizar a todos los colaboradores sobre la estrategia de seguridad de la organización y definir las líneas generales de actuación para evitar amenazas y reaccionar ante incidentes de seguridad.

Para la consecución de su objetivo, la política debe establecer directrices claras, normas para el tratamiento de la información y definir los responsables de su desarrollo, implantación y gestión. Asimismo, deberá recoger la función de "seguridad de la información" para gestionar la protección de los recursos del sistema de información.

- **Implantación de la medida**

La política deberá estar aprobada por la Dirección de la organización para evitar dudas respecto a su importancia y al compromiso de la dirección. Se deberá dar la máxima difusión

[16] [12] IBID p 49.

para que todo el personal que tenga relación con los sistemas de información de la organización conozca de su existencia y alcance[17].

El índice de la política de seguridad podría ser el siguiente:

- Alcance de la política
- Normas para el tratamiento de la información
- Responsables del desarrollo, implantación y gestión de la política
- Gestión de recursos del sistema de información

- **Normativa**

La implantación de normas sobre políticas de seguridad está reflejada en la norma ISO 27002: 2008 en los siguientes puntos:

- La dirección deberá aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información. Deberá establecer el compromiso de la Dirección y el enfoque de la Organización para gestionar la seguridad de la información. (Punto 5.1.1 ISO27002:2008)
- La política deberá tener un propietario que sea responsable de su mantenimiento y revisión, conforme a un proceso de revisión definido. (Punto 5.1.2 ISO27002:2008)

Ejemplo: Percepción de la seguridad de los usuarios del laboratorio en su trabajo diario.
Control: Definir la política de seguridad formalmente y entregarla a todos los usuarios.
Implementación: Si en el laboratorio se establecen normas de uso del sistema de información y se facilitan a todo el personal, los usuarios conocen sus responsabilidades y las posibles medidas disciplinarias en caso de incumplimiento y además se establecen controles periódicos para comprobar que las medidas descritas en la política se cumplen,

[17] [4] IBID p 13.

se contará con la colaboración de los usuarios para proteger el sistema de información.

B. CLASIFICACIÓN Y MARCADO DE LA INFORMACIÓN

No toda la información existente en la organización es igual de importante, los informes de dirección con los planes de la empresa no deben tener la misma protección que los informes de salud de los trabajadores, las copias de seguridad o las circulares para convocar reuniones. La clasificación de la información debe permitir establecer diferencias entre las medidas de seguridad a aplicar que, de forma general, atenderán a criterios de disponibilidad, integridad y confidencialidad de los datos.

Establecer un esquema de clasificación de la información debe ser riguroso y ágil a la vez, los esquemas demasiado complejos pueden ser impracticables por molestos o costosos. Con estas consideraciones se debe generar una clasificación en pocos niveles, pero que se aplique a toda la información del laboratorio, siendo recomendable considerar de forma genérica los tipos: Pública, Restringida y Confidencial.

- **Implantación de la medida**

Para diseñar un esquema de clasificación y marcado de la información, se recomiendan las siguientes actuaciones[18]:

- Establecer un sistema fácil y ágil de clasificación de la información, siguiendo las recomendaciones anteriormente citadas. Podría ser: Pública, Restringida y Confidencial.

- Definir el tratamiento de cada uno de los tipos de información, incluyendo el personal autorizado, soportes en los que se puede almacenar y usuarios o destinatarios autorizados de dicha información.

[18] [4] IBID p 13.

- Agrupar los procedimientos de clasificación de la información y tratamiento de la misma en un documento común a todo el laboratorio denominado "Guía de clasificación de la información"; esta guía deberá disponer de la aprobación de la dirección y se debe comunicar a todo el personal, tanto propio como subcontratado, que pueda tener acceso a dicha información.

- **Normativa**

La implantación de normas en clasificación y marcado de la información está reflejada en la norma ISO 17799 en el siguiente punto:

- La Información debería ser clasificada en términos de su valor, exigencias legales, sensibilidad y criticidad para la organización. (Punto 7.2.1 ISO27002:2008).

Ejemplo: El laboratorio dispone de información pública que se puede difundir fuera de la organización, e información restringida que solo debe conocer el personal de la empresa.
Control: Establecer un sistema fácil y ágil de clasificación de la información, publicar el contenido en un documento denominado Guía de Clasificación de la información.
Implementación: El laboratorio decide que la información tendrá dos niveles de clasificación: Público y Restringido, edita una guía de clasificación donde contempla los posibles casos de tratamiento de la información restringida, personal autorizado, soportes, envíos al exterior, y además, establece las medidas disciplinarias a aplicar en el caso de incumplimiento y establece controles de monitorización del cumplimiento (inventario de soportes, control de los envíos al exterior, etc.). Con estas medidas disminuye notablemente la probabilidad de error en el tratamiento de la información.

C. CONTRATOS CON TERCEROS

La evolución de los sistemas de información permite un mayor grado de subcontratación a las organizaciones, asesorías fiscales y laborales, empresas que ofrecen hosting de servidores o páginas web, copias de seguridad, entre otros, son algunos de la larga lista de servicios que se pueden contratar. Si estos terceros no conocen la política de seguridad de la organización, no

podrán ser capaces de prestar los servicios contratados con las garantías mínimas exigidas, es pues recomendable y en algún caso imprescindible, regular formalmente los servicios que involucren a personal o recursos externos a la organización.

Tratar los datos de una forma distinta a la acordada, realizar un uso de los mismos para otra finalidad distinta a la inicialmente contratada, no aplicar las medidas de seguridad exigidas, no informar a los usuarios acerca de su deber de secreto, son aspectos que deben estar perfectamente definidos al regular el contrato de prestación de servicios[19].

- **Implantación de Medidas**

Todas las relaciones con empresas y organizaciones ajenas, que impliquen el acceso a los datos e información propios de la organización deben estar reguladas mediante contrato, estos contratos deberán contemplar como mínimo:

- La identificación de todas las personas físicas y jurídicas que tendrán acceso a la información.
- La finalidad de la prestación de servicios.
- Los mecanismos de intercambio de información.
- Las medidas de seguridad a aplicar a los datos.
- La obligación de mantener el deber de secreto y de informar del mismo a todos los usuarios que puedan acceder a la información.
- Las condiciones para la finalización del contrato, incluyendo mención específica a las acciones de devolución o destrucción de la información objeto del contrato.

- **Normativa**

La redacción de contratos con terceros para la prestación de servicios a la organización está reflejada en la norma ISO 27002, en los siguientes puntos:

[19] [4] IBID p 13.

- La organización debe asegurarse de que las medidas de seguridad, servicios y niveles de entrega incluidos en los contratos de servicio con terceros, se ponen en práctica y se mantienen. (Punto 10.2.1 ISO27002:2008).

- Las exigencias para la confidencialidad y acuerdos de no divulgación, que reflejan las necesidades de la organización para la protección de la información, deberán ser identificadas y revisadas con regularidad. (Punto 6.1.5 ISO 27002:2008).

- La dirección deberá requerir a empleados, contratistas y usuarios terceros, la aplicación de las medidas de seguridad conforme a la política establecida y los procedimientos de la organización. (Puntos 8.2.1 ISO27002:2008).

- Se deberá controlar que las medidas de seguridad para el tratamiento de la información, que realizan terceros ajenos a la empresa, cumple con las exigencias de la misma. (Puntos 6.2.2 ISO27002:2008).

Ejemplo: Para la realización de las tareas contables del laboratorio, se ha decidido contratar a una empresa externa que aporta un trabajador a tiempo parcial, al que se entrega un equipo y proporciona un despacho dentro del laboratorio.
Control: Regular mediante contrato todos los encargos de tratamiento de datos y prestación de servicios con terceros que impliquen el intercambio de información.
Implementación: El laboratorio formaliza los encargos de tratamiento, redacta y firma un contrato que regula la actividad del trabajador, en el que establece las medidas de seguridad a adoptar para el tratamiento de información, las obligaciones de confidencialidad de los datos y la limitación del uso de los equipos a la finalidad recogida en el contrato.

D. CAMBIOS EN LOS CONTRATOS DE TERCEROS

Cualquier cambio en las condiciones o finalidad de los servicios contratados a terceros debe ser revisado, para comprobar que las medidas de seguridad y confidencialidad exigidas siguen vigentes. El caso concreto de la finalización de un contrato de prestación de servicios, se debe

realizar de forma ordenada y minuciosa y debe estar contemplado en la redacción del contrato que regula los servicios. Los principales aspectos que han de ser tenidos en cuenta en cualquier cambio en los servicios contratados son[20]:

- Revisión de los cambios en la finalidad de la prestación del servicio que pueden afectar a los compromisos de confidencialidad, medidas de seguridad a aplicar o condiciones del servicio.
- Revisión de los compromisos de niveles de servicio y adecuación al nuevo contrato.
- Revisión de las cláusulas de protección de datos de carácter personal.
- Revisión del deber de secreto por parte de todos los usuarios implicados en el servicio.

- **Implantación de Medidas**

Se han de verificar todos los contratos de encargo de tratamiento o prestación de servicios, para incluir las cláusulas que recojan posibles modificaciones de los mismos y verificar que existen protocolos de finalización de servicio, haciendo especial hincapié en los datos de carácter personal y/o especialmente confidenciales para el laboratorio.

- **Normativa**

Las normas sobre la finalización de contrato de servicios prestado por terceros están reflejadas, en la norma ISO 27002, en el siguiente punto:

- Los cambios en la prestación de servicios para la mejora de la política de seguridad de la organización deberán tener en cuenta lo críticos que son los sistemas de negocio y darán lugar a la reevaluación de riesgos. (Punto 10.2.3 ISO27002:2008)

Ejemplo: El laboratorio contrata el servicio de una asesoría laboral para realizar las nóminas mensuales del personal, tras dos años trabajando con dicho tercero, decide encargar la gestión laboral a otra asesoría.

[20] [4] IBID p 13.

Control: Vigilar la validez y alcance de todos los contratos de prestación de servicios para asegurar que se ajustan a la realidad del laboratorio. En caso de cambio, reflejar la nueva realidad.
Implementación: Si el laboratorio define y firma un contrato de prestación de servicios con la asesoría laboral, en el que regula el tratamiento de los datos de carácter personal y las medidas de seguridad a aplicar, se ha incluido en el contrato un protocolo de devolución de soportes en caso de finalización, al finalizar éste podrá reclamar la devolución de los soportes y encargar el servicio a un nuevo tercero.

E. COMUNICACIONES DE INFORMACIÓN CON TERCEROS

Uno de los procesos que más amenazas puede generar en las relaciones con los terceros es el intercambio de información. El envío de datos a través de soportes como USB, CD-ROM o redes de telecomunicaciones como correo electrónico, mensajería, generan amenazas a la integridad de los datos, pero también a la confidencialidad de los mismos. Evitar pérdidas, intercepciones o alteraciones de la información, es una prioridad para la organización.

- **Implantación de Medidas**

Los procesos de comunicación deben estar perfectamente definidos y regulados en los contratos de prestación de servicios. De forma adicional, se deben establecer normas y mecanismos que permitan realizar comunicaciones de información de forma segura, dentro de la organización y con terceros. Dichas normas deben estar recogidas formalmente y ser difundidas a todos los implicados en el envío o recepción de información[21].

- **Normativa**

La necesidad de definir e implantar normas sobre la comunicación de información con terceros está reflejada en la norma ISO 27002, en el siguiente punto:

[21] [4] IBID p 13.

- Se debe establecer procedimientos y normas formales para proteger el intercambio de información, así como los mecanismos de comunicación empleados. (Punto 10.8.1 ISO27002:2008)

Ejemplo: El laboratorio, en virtud del contrato de prestación de servicios firmado con la asesoría laboral, envía por mail los datos de los nuevos empleados contratados a la asesoría, y recibe del mismo modo los contratos y las nóminas dirigidos al departamento de administración. Una vez recibidas, las nóminas se imprimen y se entregan en papel al departamento financiero.
Control: Regular los intercambios de información con terceros formalmente, comunicando los requisitos al personal de la organización y a los terceros involucrados en dichos intercambios.
Implementación: Si el laboratorio decide establecer normas y medidas de seguridad para proteger las comunicaciones, estas se deben documentar en un procedimiento y ser comunicadas a todos los afectados. A modo de resumen, las normas definidas son: - En el envío de información entre la empresa y la asesoría laboral, todos los mensajes deberán ir firmados y cifrados, siendo eliminados todos aquellos que no lo estén. - Una vez recibidas las nóminas por el departamento de administración, se confirmará su recepción a la asesoría y se procederá a su impresión y a la destrucción del mail recibido. - La entrega de las nominas en papel desde el departamento de administración y su correspondiente recepción por parte del departamento financiero, se realizará siempre mediante la introducción de dichas nóminas en un sobre sellado, que será transportado por personal autorizado por el responsable del departamento de administración.

6.3.3.2 CONTROLES RELACIONADOS CON EL PERSONAL[22]

El personal que maneja el sistema de información, es uno de los elementos principales en el análisis de medidas de seguridad de la información, de su colaboración depende en buena medida el éxito o fracaso de muchas de las medidas de seguridad a implantar. A continuación se establecerán aquellas medidas que inciden de forma esencial sobre el personal, ya sea respecto al uso que hacen de los sistemas de información, manejo de incidencias de seguridad o normas de seguridad a aplicar.

A. DEFINICIÓN DE FUNCIONES Y RESPONSABILIDADES

Una de las principales amenazas de toda el laboratorio es el acceso de usuarios no autorizados (internos o externos) que puedan consultar, modificar, borrar e incluso robar información a la que no deberían acceder. El usuario del sistema de información debe ser informado de forma clara y precisa acerca de sus funciones y obligaciones en el tratamiento de los datos.

- **Implantación de Medidas**

Se deben definir las funciones y responsabilidades de seguridad para cada uno de los usuarios del sistema de información; para ello se aplicará el principio de establecer los mínimos privilegios necesarios para el desarrollo de dichas labores. Cada proceso de seguridad debe identificar a un propietario y a los usuarios que participarán en el mismo. De esta forma se evitarán malentendidos acerca de las responsabilidades sobre los elementos del sistema de información. Todas las funciones y responsabilidades deben comunicarse a los usuarios involucrados en su ejecución, de una forma clara y asegurando su recepción y entendimiento. Se prestará especial atención al tratamiento de datos de carácter personal[23].

- **Normativa**

La definición de funciones y responsabilidades del personal con acceso a datos está regulada en la norma ISO 27002, en el siguiente punto:

[22] NTC-ISO/IEC 27005, Tecnología de la información. Código de práctica para la gestión de la seguridad de la información.
[23] [4] IBID p 13.

- Las funciones de seguridad y las responsabilidades de los empleados, contratistas y usuarios terceros, deben estar definidas y documentadas conforme a la política de seguridad de la información de la organización. (Punto 8.1.1 ISO27002:2008).

Ejemplo: Un usuario es contratado por el laboratorio para hacerse cargo de la Recepción; entre sus funciones está atender todas las solicitudes de muestreo que llegan al laboratorio y pasarlas con el departamento correspondiente. Para la gestión de las solicitudes de muestreo se le facilita un equipo con acceso al sistema de tratamiento de la empresa.
Control: Definir las funciones y responsabilidades de todo el personal formalmente, comunicarlas a los usuarios de una forma clara y asegurando su recepción y entendimiento.
Implementación: En una empresa en la que se informa al usuario sobre sus funciones en la empresa, sus responsabilidades y las posibles medidas disciplinarias en caso de incumplimiento de las mismas, quedando constancia formalmente de que ha recibido dicha información. - Se limita su acceso dentro del sistema de información a un nivel adecuado para el desarrollo de sus funciones. - Se auditan los intentos de acceso de cada usuario a recursos a los que no está autorizado. - Esta persona se limita a atender las solicitudes de muestreo y remitirlas al departamento correspondiente.

B. CLÁUSULAS DE CONFIDENCIALIDAD

Además de la información de qué datos tratar y de qué forma, todo usuario debe recibir información acerca de la obligación de mantener secreto profesional sobre los datos que conozca en el desarrollo de sus funciones, aún después de finalizar la relación laboral que le une a la organización. El usuario debe firmar un acuerdo de confidencialidad, en el que se informe de sus funciones y obligaciones respecto a la información de la organización.

- **Implantación de Medidas**

Se deben definir exigencias de confidencialidad y no divulgación de datos para todo el personal que dispone de acceso al sistema de información para el desarrollo de sus funciones, tanto para el personal contratado como para el personal externo. Estas exigencias se definirán formalmente en acuerdos de confidencialidad, que todo el personal deberá firmar como prueba de su recepción[24].

- **Normativa**

La confidencialidad del personal con acceso a datos está regulada en la norma ISO 27002 en el siguiente punto:

- Las exigencias de confidencialidad y acuerdos de no divulgación, que reflejan las necesidades de la organización en materia de protección de información, deberán ser identificadas y revisadas regularmente. (Punto 6.1.5 ISO27002:2008).

Ejemplo: Se contrata una persona temporalmente para la realización de las tareas de analista, para suplir una baja temporal del usuario encargado de dichas funciones; durante este tiempo esa persona accede a todos los procedimientos del laboratorio.
Control: Se definirán cláusulas de información sobre el deber de secreto y confidencialidad de los datos que todos los usuarios con acceso al sistema deberán firmar.
Implementación: En el contrato se incluye una cláusula de confidencialidad con los datos que trate, estableciendo las medidas legales y disciplinarias en el caso de incumplimiento de esta confidencialidad. - Antes de ofrecer y comentar información sobre la empresa lo piensa dos veces, ya que asume las medidas legales y disciplinarias establecidas en el contrato. - En el caso de sustracción o vulneración de dicha confidencialidad, el laboratorio podría emprender medidas legales contra él.

[24] [4] IBID p 13.

C. CONCIENCIACIÓN Y EDUCACIÓN SOBRE NORMAS DE SEGURIDAD

Para que los usuarios puedan colaborar con la gestión de la seguridad, se les debe concienciar e informar a fin de que cumplan con las medidas establecidas por el laboratorio en el desempeño habitual de sus funciones. Es preciso instruir al personal de forma apropiada sobre seguridad y el uso correcto de los sistemas de información y sus recursos, así como sobre la importancia de la seguridad en el tratamiento de los datos en la organización.

- **Implantación de Medidas**

Se debe formar a todo el personal de la empresa que vaya a tratar datos del sistema de información sobre las normas de utilización y medidas de seguridad que debe contemplar dicho tratamiento. Conseguir que todo usuario conozca las instrucciones para tratar los recursos, la respuesta ante incidencias de seguridad y el mantenimiento de los recursos, es una forma de disminuir los errores de tratamiento y los malos usos de los recursos del sistema de información[25].

- **Normativa**

La regulación sobre la formación y concienciación del personal con acceso a datos está regulada en la ISO 27002, en el siguiente punto:

- La organización deberá identificar y revisar las necesidades de confidencialidad y recogerlas en acuerdos de no divulgación. (Punto 6.1.5 ISO27002:2008)

Ejemplo: Se contratan dos trabajadores para introducir las solicitudes de nuevos clientes en el sistema de información, e informarles sobre los servicios que ofrece la empresa. Se les facilita un equipo para la ejecución de sus funciones.
Control: Se concienciará y formará al personal sobre la importancia de la aplicación de las medidas de seguridad definidas por la organización en el correcto desempeño de sus

[25] [4] IBID p 13.

funciones.
Implementación: Antes de iniciar el trabajo se forma a los trabajadores sobre el uso de las aplicaciones y recursos del sistema, se les comunica una forma común para la introducción de clientes con el formato apellidos y nombre, se les comunica que las ofertas se almacenan en una carpeta común en el servidor, y se les indica un procedimiento para reportar incidencias en los equipos o en el tratamiento de información; además se les informa sobre la legislación aplicable en materia de protección de datos de carácter personal. - Ambas encuentran los clientes correctamente. - No se envía información duplicada a los clientes, ya que ambas disponen de un repositorio común de información. - Todas las incidencias son estudiadas ayudando a mejorar el sistema de información. - Se evita el riesgo de incumplimientos legales.

D. ESCRITORIO LIMPIO Y SEGURIDAD DE EQUIPO DESATENDIDO

El escritorio del equipo informático y el entorno de trabajo son dos elementos del sistema de información cuyo uso inapropiado puede generar amenazas sobre la confidencialidad de los datos, tales como acceso a información confidencial por personas no autorizadas o robos de información.

- **Implantación de Medidas**

Se deben establecer normas y mecanismos para que el personal tenga el escritorio sin información visible que pueda comprometer la confidencialidad de los datos, de igual forma la mesa de trabajo debe estar libre de documentos confidenciales. Se debe adoptar una política de escritorio limpio de papeles y medios de almacenamiento extraíbles, una política de pantalla

limpia para las aplicaciones informáticas, así como normas de seguridad para proteger la información cuando el usuario abandona el entorno de trabajo[26].

- **Normativa**

La implantación de normas sobre escritorio limpio y establecimiento de normas de seguridad para los equipos desatendidos están reguladas en la norma ISO 27002, en los siguientes puntos:

- Los usuarios deben asegurar que el equipo desatendido tiene la protección apropiada. (Punto 11.3.2 ISO27002:2008)
- Se debe definir una política de escritorio limpio de papeles y medios de almacenamiento extraíbles, así como una política de pantalla limpia para las aplicaciones informáticas. (Punto 11.3.3 ISO27002:2008)

Ejemplo: Un miembro del personal, encargado de la preparación de los informes de resultados del laboratorio, dispone de un certificado digital instalado en su equipo para las comunicaciones con los clientes y chequeo de pagos por medio de banca on line a través de Internet.
Control: Se definirán normas de abandono del puesto de trabajo y gestión del escritorio que se comunicarán a los usuarios formalmente.
Implementación: En la mesa de trabajo el empleado sólo tiene documentos públicos, guarda bajo llave las validaciones de los pagos por Internet y los informes de resultados. Cuando deja el equipo desatendido bloquea el equipo para que solo su usuario pueda desbloquearlo. La entrega de los informes de resultado se realiza mediante un sobre cerrado.

E. RESPONSABILIDAD EN EL USO DE CONTRASEÑAS

[26] [4] IBID p 13.

En la actualidad, la mayoría de los sistemas de información utilizan sistemas de autenticación de usuarios basados en contraseñas, limitando el acceso a los recursos del sistema según el perfil de trabajo al que pertenece el usuario. Diariamente se recibe información sobre amenazas, como suplantación de identidad de los usuarios, acceso no autorizado a los sistemas de información, acceso no autorizado a datos, etc., que forman parte de la realidad cotidiana en las empresas. La principal estrategia para que los usuarios utilicen sus contraseñas en el sistema de forma segura, es formarlos sobre su correcto uso.

- **Implantación de medidas**

La entrega de las credenciales al usuario (nombre de usuario y contraseña) debe realizarse por algún procedimiento que obligue al usuario a cambiar la contraseña en el siguiente inicio de sesión, lo que garantiza que solamente él conoce la contraseña. Se debe formar a los usuarios en la selección y empleo de sus contraseñas, para garantizar que las mismas tienen una calidad mínima frente a intentos de acceso. Se debe concienciar a los usuarios de la confidencialidad de la contraseña, y de que la revelación de la misma supone una suplantación de su identidad digital, que puede tener repercusiones disciplinarias y legales[27].

- **Normativa**

Las medidas sobre la responsabilidad de los usuarios en el uso de sus contraseñas están reguladas en la ISO 27002, en los siguientes puntos:

Se debe requerir a los usuarios buenas prácticas de seguridad en la selección y empleo de sus contraseñas. (Punto 11.3.1 ISO 27002:2008)

- La asignación de contraseñas debería ser controlada por un proceso de dirección formal. (Punto 11.2.3 ISO 27002:2008)

- Todos los usuarios deberían tener un identificador único para su empleo personal y una técnica conveniente de autenticación debería ser escogida para justificar la seguridad de identificación de los usuarios. (Punto 11.5.2 ISO27002:2008)

[27] [4] IBID p 13.

- Los sistemas de contraseñas deberán asegurar la calidad de las mismas. (Punto 11.5.3 ISO 27002:2008)

Ejemplo: El administrador del sistema de información se encarga de la asignación de las contraseñas de acceso al sistema de información del personal y las comunica por escrito.
Control: Se deberá seleccionar un procedimiento de asignación de contraseñas así como concienciar y formar a los usuarios sobre la importancia de la confidencialidad de las contraseñas y sobre la elección de contraseñas robustas.
Implementación: El laboratorio establece normas sobre la responsabilidad de los usuarios en el uso de sus contraseñas y les informa formalmente. Los usuarios memorizan sus contraseñas o las guardan en un lugar donde sólo ellos pueden acceder. El administrador obliga a cambiar la contraseña a los usuarios la primera vez que inician sesión, quedando esta únicamente en conocimiento de dicho usuario. - Sólo ese usuario tendrá acceso al sistema de información con su nombre de usuario y contraseña. - Si se garantiza que las pruebas no son alterables, las actuaciones del usuario podrán tener carácter probatorio de sus acciones.

F. NORMAS DE SEGURIDAD EN CORREO ELECTRÓNICO

El uso del correo electrónico genera importantes amenazas al sistema de información. Infección de equipos por malware, envíos de información sin las medidas de seguridad correctas o sustracción de información son algunas amenazas.

- **Implantación de Medidas**

Deben establecerse normas de seguridad para el uso del correo electrónico, que recojan las medidas de seguridad mínimas para garantizar un uso responsable y seguro del servicio. La

Información confidencial enviada a través de mensajería electrónica deberá estar protegida de manera apropiada, para que ningún tercero no autorizado pueda tener acceso a la misma[28].

- **Normativa**

La implantación de normas sobre seguridad en el uso del correo electrónico está reflejada en la norma ISO 17799 en el siguiente punto:

- La Información confidencial enviada a través de mensajería electrónica debería ser protegida de manera apropiada. (Punto 10.8.4 ISO27002:2008)

Ejemplo: En el laboratorio se facilita a todos los usuarios una cuenta de correo electrónico y se configura en sus equipos.
Control: Se debe restringir el uso del correo electrónico a aquellos usuarios autorizados expresamente. Los usuarios autorizados deberán recibir formación complementaria con especial atención a las posibles amenazas que pueden presentar.
Implementación: el laboratorio facilita formalmente al personal las normas de seguridad para manejar el correo electrónico. "No abrir correos sospechosos, de direcciones desconocidas o con asuntos poco fiables", "no abrir ningún archivo adjunto sin antes analizarlo con un antivirus", "no enviar información confidencial sin cifrado", son aspectos recogidos en dichas normas.

G. FORMACIÓN SOBRE MANEJO DE INCIDENCIAS

La formación de los usuarios sobre el manejo de incidencias es fundamental para mantener y gestionar correctamente el sistema de información de la organización. Sin una adecuada política de manejo de incidencias, los tiempos de mantenimiento se alargan y los problemas de seguridad se incrementan, sin dar lugar a acciones inmediatas para su solución.

- **Implantación de Medidas**

[28] [4] IBID p 13.

Deben existir canales establecidos para informar, lo más rápidamente posible, de los incidentes relativos a la seguridad y al mal funcionamiento de los sistemas de información. Todos los empleados de la organización, incluidos los externos, deben conocer los procedimientos de comunicación de incidencias, así como las infracciones en materia de seguridad que pueden tener un impacto en la seguridad de los activos de información. La formación ayudará a la hora de localizar, resolver y analizar las incidencias que ocurren en el sistema de información de la empresa, antes de que el daño producido pueda extenderse o agravarse[29].

- **Normativa**

Existe regulación sobre la formación sobre incidencias del personal con acceso a datos en la norma ISO 27002, en el siguiente punto:

- Se deben establecer procedimientos documentados de comunicación formal de incidencias de seguridad. Todos los empleados, contratistas y usuarios terceros deben conocer dichos procedimientos, para identificar los distintos tipos de incidencias y debilidades que podrían tener un impacto sobre la seguridad del sistema de información de la organización. Se debe requerir que ellos comuniquen cualquier incidencia de seguridad de la información, tan rápidamente como sea posible, al punto de contacto designado. (Punto 13.1 ISO27002:2008)

Ejemplo: Un usuario sufre el bloqueo de su equipo informático mientras realiza sus funciones, y decide apagarlo y volverlo a encender cada vez que le ocurre.
Control: Se debe definir un procedimiento de gestión de incidencias de seguridad y entregar a cada usuario sus obligaciones para el adecuado cumplimiento del mismo.
Implementación: En la empresa, se informa a todo el personal con acceso al sistema de información, sobre el procedimiento a seguir si se detecta cualquier fallo o incidencia en

[29] [4] IBID p 13.

el sistema de tratamiento de información. De este modo, la detección de incidencias alcanzará a todos los usuarios del laboratorio y permitirá su correcta gestión y solución.

6.3.3.3 CONTROLES RELACIONADOS CON LOS SISTEMAS DE INFORMACIÓN[30]

El sistema de información empleado, así como su configuración y gestión, es otro de los factores cuyo análisis resulta imprescindible para crear una adecuada estrategia de seguridad de la información. Los controles a considerar se pueden agrupar en físicos y lógicos. Los controles físicos contemplan aquellos elementos relacionados con el entorno (como pueden ser los locales), o con los soportes (como pueden ser los discos duros, el papel…) y los controles lógicos agrupan los sistemas (como pueden ser las aplicaciones, las copias de datos, etc.) y las comunicaciones (como pueden ser redes locales, conexiones desde el exterior, etc.). Es preciso definir normas de funcionamiento y uso para todos ellos.

6.3.3.3.1 SEGURIDAD FÍSICA RELACIONADA CON EL ENTORNO

La primera barrera para el acceso al sistema de información de la organización es el acceso físico. Protegiendo el acceso a los locales se protege el acceso físico al sistema de información. Establecer un perímetro físico, controles físicos de entrada a los locales o en las zonas de carga y descarga, son las primeras medidas de seguridad a recoger en el sistema.

A. PERÍMETRO FÍSICO DE SEGURIDAD Y CONTROLES DE ACCESO

Los mecanismos de protección para el sistema de información de la organización pasan por definir un perímetro físico de seguridad que impida el acceso no autorizado a la información. Una vez establecido un perímetro de seguridad, se debe regular el acceso físico a dicho perímetro; para ello, se deben establecer controles físicos de seguridad de entrada a los locales y a las ubicaciones que permitan un acceso al sistema de información.

[30] [22] IBID p 61.

- **Implantación de Medidas**

Establecer un perímetro físico de seguridad que proteja la información de la organización es vital para prevenir incidencias. El perímetro físico es la primera barrera de protección del sistema de información que garantiza en gran medida el funcionamiento del resto de medidas. El acceso al local, mediante vías de acceso autorizadas y controladas, barreras arquitectónicas como paredes o ventanas, elementos adicionales como áreas de descarga controladas, debe ser gestionado para proteger las zonas que contienen instalaciones informáticas o permiten el acceso a las mismas. Dentro del perímetro de seguridad, se deben identificar las ubicaciones que almacenan soportes que puedan contener datos confidenciales o especialmente protegidos (en el caso de datos de carácter personal); estas ubicaciones dispondrán de una identificación personal de los usuarios que permita validar que disponen de autorización para el acceso. Se deben validar las medidas de seguridad físicas de acceso al perímetro de seguridad, compuestas por puertas, cerraduras, alarmas, vigilancia, etc., y formalizarlas en instrucciones de acceso al laboratorio, que deberán ser comunicarlas a todo el personal[31].

- **Normativa**

La implantación de normas sobre seguridad en la definición de un perímetro físico de seguridad y controles físicos de entrada al mismo está reflejada en la norma ISO 27002, en los siguientes puntos:

- Perímetros de Seguridad (barreras como paredes, tarjeta de control puertas de entrada o control en los escritorios de recepción) deberían ser usados y proteger las áreas que contienen instalaciones informáticas e información. (Punto 9.1.1 ISO27002:2008)

- Las áreas seguras deberán estar protegidas por controles de entrada apropiados, para asegurar que permiten el acceso sólo al personal autorizado. (Punto 9.1.2 ISO27002:2008)

- La seguridad física para oficinas, cuartos e instalaciones deberá ser diseñada y aplicada. (Punto 9.1.3 ISO27002:2008)

[31] [4] IBID p 13.

Ejemplo: El laboratorio dispone de un cuarto de enfriamiento para el almacenamiento de las muestras.
Control: Se debe definir un perímetro de seguridad que represente la primera barrera de acceso a los sistemas de información. Se definirán las normas de acceso al interior de dicho perímetro para personal autorizado. Dichas normas serán difundidas y de obligado cumplimiento.
Implementación: La empresa delimita como perímetro de seguridad la ubicación del cuarto frio, establece medidas de restricción de acceso y asegura puertas y ventanas e informa a todo el personal de sus funciones.

B. CONTROL DE ACCESOS PÚBLICOS, ÁREAS DE CARGA Y DESCARGA

Las áreas de carga y descarga de mercancías, los accesos públicos y los accesos de entrega de material a las oficinas de la organización, suponen amenazas de accesos no autorizados y por tanto, requieren de un tratamiento específico respecto a las medidas de seguridad a implantar.

- **Implantación de Medidas**

De forma habitual, un laboratorio necesita elementos de comunicación con el exterior, estos elementos o espacios permiten el tránsito de mercancías y personas y suponen de una forma manifiesta amenazas a la seguridad. Se deben definir normas de uso de dichos espacios, de forma que en ningún momento queden desatendidos de personal de la organización que vigile los posibles accesos que puedan producirse desde estos elementos. Las medidas de seguridad aplicables a estos espacios pueden ir, desde puertas blindadas, alarmas, sistemas de seguridad profesionales con vigilancia 24h, etc[32].

- **Normativa**

[32] [4] IBID p 13.

La implantación de normas sobre seguridad en el control de los accesos públicos, áreas de carga y descarga o áreas de entrega, están reflejadas en la norma ISO 27002 en el siguiente punto:

- Los puntos de acceso a la organización tales como zonas de entrega de mercancías, áreas de carga y descarga y otros puntos donde personas no autorizadas pueden entrar sin permiso deben ser controlados y, de ser posible, aislados de las instalaciones informáticas y sistema de información de la empresa para así evitar el acceso no autorizado. (Punto 9.1.6 ISO27002:2008)

Ejemplo: El laboratorio dispone de un área de carga y descarga de mercancías en la que existe un acceso a la recepción, también existe un acceso desde el exterior para clientes y proveedores.
Control: Se debe establecer un adecuado control de los espacios de acceso público y áreas de carga y descarga, normalizar los accesos a dichas zonas y vigilar su correcto cumplimiento.
Implementación: En el laboratorio se definen y cumplen las siguientes medidas: - Los accesos desde el área de carga y descarga están controlados mediante una puerta cerrada, que solo se puede abrir mediante un código, y sólo el personal autorizado dispone de código de apertura. - Los accesos públicos permanecen cerrados y existe una persona encargada de abrir dichos accesos a terceros. - Los terceros que tengan que acceder a las oficinas para la entrega de alguna documentación siempre son acompañados por personal autorizado. - Estas normas de seguridad se formalizan y se entregan al personal encargado de la vigilancia y descarga de mercancías.

C. PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES

La mayor parte de las amenazas externas y ambientales no son controlables por parte de la organización, en su análisis se deben definir medidas de seguridad para evitar impactos en la organización, tales como la pérdida total o parcial del sistema de información de la empresa.

- **Implantación de Medidas**

Estas medidas están condicionadas en su mayor parte por los requisitos de negocio establecidos al analizar los principales riesgos de la organización. Ver Figura C.

- **Normativa**

La implantación de normas sobre protección contra amenazas externas y ambientales están reflejadas en la ISO 17799 en el siguiente punto:

- La protección física contra el daño del fuego, inundación, terremoto, explosión, terceros malintencionados y otras formas de desastre natural o artificial debería ser diseñada y aplicada. (Punto 9.1.4 ISO27002:2008)

Ejemplo: El laboratorio está ubicado en los márgenes del río Bogotá.
Control: Se debe establecer un Plan anti desastres naturales que garantice la recuperación de los sistemas en caso de desastre.
Implementación: El laboratorio decide establecer un sistema de evacuación de emergencia e instruir al personal sobre las tareas a llevar a cabo en caso de inundación.

6.3.3.3.2 SEGURIDAD FÍSICA RELACIONADA CON LOS SOPORTES[33]

Todos los activos de la compañía se deben inventariar, etiquetar y clasificar según su sensibilidad e importancia todo esto debe tener un responsable con el fin de manejar control en la información como nivel de protección a la seguridad.

[33] [4] IBID p 13.

A. INVENTARIO Y ETIQUETADO DE SOPORTES

Incluido en la "Guía de clasificación de la información", se debe definir la forma de identificar el tipo de información que contiene cada uno de los diferentes soportes utilizados en la organización. Estos procedimientos de tratamiento de la información deben cubrir tanto los formatos físicos como los formatos lógicos, incluyendo para cada tipo: Copia, Almacenamiento, Transmisión por correo, fax y correo electrónico, Transmisión oral, incluida telefonía móvil, transmisión de voz y máquinas de respuesta automática, Destrucción[34].

El etiquetado de la información puede realizarse de diferentes formas, pero se debería hacer de manera que se distinga de una forma fácil el tipo de información que contiene el documento. El inventario de soportes permitirá llevar una mejor gestión de la información, controlando en todo momento los tratamientos y salidas de información fuera de la organización.

- **Implantación de Medidas**

Tras la aprobación por la dirección la Guía de clasificación de información, se dispone del respaldo necesario para abordar el inventario y etiquetado de soportes. Una vez seleccionado el procedimiento de etiquetado, se procederá a identificar en el inventario todos los soportes y a etiquetarlos según el contenido que almacenan o tratan. Dicho inventario será mantenido de forma periódica, según los requisitos establecidos en la Guía de clasificación de la información.

- **Normativa**

La implantación de normas sobre inventariado y etiquetado de soportes está reflejada en la ISO 27002 en los siguientes puntos:

- Todo activo del sistema de información debería ser claramente identificado e inventariado. (Punto 7.1.1 ISO27002:2008)

[34] [4] IBID p 13.

- Un apropiado juego de procedimientos para el manejo y etiquetado de la información debería ser desarrollado y puesto en práctica conforme al esquema de clasificación adoptado por la organización. (Punto 7.2.2 ISO27002:2008)

Ejemplo: El laboratorio no ha etiquetado los soportes ni dispone de inventario.
Control: Se debe crear un inventario de soportes y proceder a su etiquetado de acuerdo a las normas recogidas en la Guía de clasificación de la información.
Implementación: El laboratorio publica y comunica a todos los trabajadores una Guía de clasificación de la información. Cada soporte dispone de una etiqueta identificativa y está relacionado en el inventario de soportes. Se custodian con medidas especiales aquellos soportes que almacenan información restringida. Se crea un procedimiento para revisar la conformidad del inventario mensualmente. - Se pueden detectar posibles pérdidas o sustracciones de soportes - Es más fácil catalogar y aplicar medidas de seguridad a los soportes

B. SALIDAS DE SOPORTES CON DATOS DE LAS INSTALACIONES

Una vez inventariados y etiquetados los soportes, se debe controlar cualquier movimiento de los mismos fuera del perímetro de seguridad establecido en las instalaciones del laboratorio.

- **Implantación de Medidas**

Para cumplir con el control de la salida de soportes se deberá establecer un registro que incluya: la identificación del soporte que sale de la organización, la autorización por parte del responsable encargado de su supervisión, el destino del soporte, la fecha y hora del envío y la finalidad del mismo.

- **Normativa**

La implantación de procedimientos que controlan las salidas de soportes con datos de las instalaciones de la empresa está reflejada en la norma ISO 27002, en el siguiente punto:

- Los equipos, la información o el software no deberán salir fuera de los locales de la empresa sin autorización previa. (Punto 9.2.7 ISO27002:2008)

Ejemplo: El laboratorio entrega a un proveedor un material para realizar un prototipo y no hay constancia del soporte de salida.
Control: Se debe crear un registro de salida y entrada de soportes que permitan identificar el soporte, la finalidad del movimiento, la fecha y hora, la autorización del responsable y el destino del mismo, como requisitos mínimos.
Implementación: En la empresa se solicita una autorización por escrito para sacar cualquier soporte de las instalaciones, se realizan comprobaciones de las medidas de seguridad antes de salir y se refleja dicha salida en un registro. Con estas actuaciones, la empresa tiene controladas las salidas de soportes que se realizan en sus instalaciones, así como las medidas de seguridad aplicadas a las mismas.

C. MEDIDAS DE REUTILIZACIÓN / ELIMINACIÓN DE SOPORTES

Los soportes que se reutilizan o eliminan, deben ser objeto de un proceso de eliminación o borrado de los datos que almacenan, para evitar posteriores accesos no autorizados a la información que contienen. El proceso de borrado, deberá quedar registrado en el inventario de soportes indicando la fecha y hora, el responsable que lo ha realizado y la nueva finalidad del soporte.

- **Implantación de Medidas**

Se deben definir procedimientos formales que definan las medidas de seguridad para la reutilización y eliminación de los soportes del sistema de información de la empresa. Medidas como la eliminación total y segura de los datos de todos los soportes antes de su reutilización,

o la destrucción física de los mismos para su desecho, se deben implantar formalmente en la organización[35].

- **Normativa**

La implantación de medidas de reutilización / eliminación de soportes está reflejada en la norma ISO 27002 en el siguiente punto:

- Los soportes que almacenen datos deberán ser eliminados de modo seguro cuando se desechen, usando para ello procedimientos formales. (Punto 10.7.2 ISO27002:2008)

Ejemplo: Se compra un computador nuevo para el responsable de los informes de resultados del laboratorio, dejando el equipo antiguo al nuevo trabajador del área de mantenimiento.
Control: Se deben establecer procesos formales de eliminación y reutilización de soportes que garanticen la confidencialidad de la información almacenada en ellos.
Implementación: El laboratorio decide definir las medidas de reutilización y desecho de los soportes de la empresa. Antes de cambiar de ubicación el equipo se procede a la eliminación de toda la información del disco duro del equipo. Con estas medidas se impide el acceso a los datos que contenían los soportes antes de su reutilización o desecho.

D. NORMAS DE USO DE DISPOSITIVOS MÓVILES Y SOPORTES EXTRAÍBLES

Los dispositivos móviles, así como los soportes extraíbles generan vulnerabilidades en la seguridad del sistemas de información, debido a su facilidad de uso, alta movilidad, capacidad de almacenamiento y políticas permisivas por parte de las organizaciones, que permiten el flujo de información albergada en los soportes sin control alguno.

- **Implantación de Medidas**

[35] [4] IBID p 13.

Las actuaciones para conseguir un control sobre el uso de dispositivos móviles y soportes extraíbles contempla la realización de una clasificación de la información, que incluya la identificación de los soportes y la información que almacena. Se deben realizar las siguientes actuaciones[36]:

- Inventariar todos los soportes existentes, asignando a cada uno de ellos un responsable.
- Etiquetar de forma visible cada soporte, según las normas recogidas en la guía de clasificación de la información.
- Prohibir la creación y uso de soportes no autorizados que no dejen registro en el inventario de la organización.
- Establecer instrucciones de uso de cada tipo de dispositivo móvil o soportes, incluyendo los usuarios autorizados, entradas y salidas de la organización y la notificación de las incidencias que puedan presentarse en materia de seguridad de la información.
- **Normativa**

La implantación de normas de uso de soportes extraíbles está reflejada en la norma ISO 27002 en el siguiente punto:

- Debería haber procedimientos que describan las medidas de seguridad para el manejo de medios extraíbles. (Puntos 10.7.1 ISO17799:2005)

Ejemplo: El laboratorio decide que facilitará al responsable del departamento de calidad una memoria USB, para la realización de las copias de seguridad de los resultados del laboratorio.
Control: Se deben establecer normas de uso de dispositivos móviles y soportes extraíbles que garanticen la confidencialidad de la información almacenada en ellos.
Implementación: El laboratorio define normas de uso de la USB, la etiqueta como

[36] Ibid p75.

almacén de información Restringida, lo refleja en el inventario de soportes y lo entrega al usuario responsable del mismo. Al mismo tiempo, se definen las normas de uso del soporte, que incluyen medidas disciplinarias en caso de incumplimiento de las mismas, entregándoselas por escrito al responsable del departamento de calidad. Dentro de las normas también se incluye la información de que periódicamente, sin aviso, se le podrá solicitar que entregue el soporte para comprobar que dichas normas de uso se cumplen correctamente. Todas las medidas quedan reflejadas formalmente mediante un escrito firmado.

E. MANTENIMIENTO DE EQUIPOS

El mantenimiento de los equipos afecta directamente a la seguridad del sistema de información, fallos en los discos de almacenamiento de datos pueden originar pérdidas de información, por lo que se debe llevar un control del mantenimiento de todos los equipos y soportes que componen el sistema de información de la empresa.

- **Implantación de Medidas**

Los equipos del sistema de información se deben mantener adecuadamente para asegurar su disponibilidad dentro del sistema de información, para ello existen recomendaciones de mantenimiento especificadas por el fabricante, que se deben seguir siempre que sea posible. El mantenimiento debe realizarlo personal cualificado y se debe llevar un control de todas las actuaciones realizadas en el sistema. Las incidencias de seguridad, debidas a errores o defectos de los equipos o del mantenimiento, deberán ser documentadas y formar parte de posibles reclamaciones al fabricante[37].

- **Normativa**

La implantación de procedimientos de mantenimiento de equipos del sistema de información está reflejada en la norma ISO 27002 en el siguiente punto:

[37] [4] IBID p 13.

- Los equipos informáticos deberán ser mantenidos correctamente para asegurar su disponibilidad e integridad continuada. (Punto 9.2.4 ISO27002:2008)

Ejemplo: El laboratorio cuenta con varios equipos informáticos dentro de su sistema de información.
Control: Se deben establecer procedimientos de mantenimiento de equipos y garantizar que son ejecutados por personal cualificado de forma periódica.
Implementación: Se consulta con la empresa que ha instalado los equipos y se establece que los equipos deberían pasar, como mínimo una revisión anual, para comprobar que todos los componentes funcionan correctamente, por lo que la empresa documenta y acuerda formalmente con la empresa la revisión anual de todos los equipos. Con esta medida la empresa disminuye la posibilidad de daños en el hardware de los equipos de su sistema de información.

F. PROTECCIÓN CONTRA FALLOS EN EL SUMINISTRO ELÉCTRICO

El suministro eléctrico es fundamental para el funcionamiento del sistema de información, errores en el diseño del sistema eléctrico de alimentación, en la aplicación de controles para estabilizar la corriente de entrada, o en la dimensión de los sistemas de respaldo, pueden dar lugar a pérdidas de horas de trabajo y de información.

- **Implantación de Medidas**

Se debe realizar un diseño adecuado del sistema de suministro eléctrico por profesionales, incluyendo sistemas que estabilicen la tensión suministrada a los equipos y sistemas de respaldo para suministrar energía en caso de fallo en el suministro[38].

- **Normativa**

[38] [4] IBID p 13.

La implantación de medidas de protección contra fallos del suministro eléctrico está reflejada en la norma ISO 27002 en el siguiente punto:

- Los equipos deberán estar protegidos ante posibles fallos de suministro eléctrico y otras interrupciones relacionadas. (Punto 9.2.2 ISO27002:2008)

Ejemplo: Daños en los sistemas informáticos por cortes de suministro o altibajos de tensión.
Control: Se debe diseñar un sistema de suministro eléctrico, incluyendo medidas de respaldo, acorde a las necesidades del sistema de información y revisarlo en función de los cambios introducidos en el mismo.
Implementación: El laboratorio decide instalar un sistema estabilizador para todo el sistema informático, se documenta dicho sistema y las normas para que sólo el material informático de tratamiento de datos sea conectado a dicho sistema. Con esta medida se previenen los posibles cortes de suministro y variaciones bruscas de tensión.

6.3.3.3.3 SEGURIDAD LÓGICA EN LOS SISTEMAS[39]

A. ANÁLISIS DE NECESIDADES PARA EL SOFTWARE

La adquisición de software para la organización debe ser fruto de un estudio de necesidades, que incluya los requisitos mínimos que la organización quiere garantizar en materia de seguridad de la información.

- **Implantación de Medidas**

Como paso previo a la adquisición de cualquier software, se deben analizar los requisitos de seguridad del sistema de información corporativo, este paso evitará amenazas de seguridad

[39] [22] IBID p 61.

respecto a la identificación de usuarios, defectos en las medidas de seguridad o registros de incidentes, etc.

- **Normativa**

La implantación de procedimientos de análisis de necesidades para el software de tratamiento de información está reflejada en la norma ISO 27002 en el siguiente punto:

- Se deberán estudiar las exigencias de negocio para nuevos sistemas de información o mejoras de los sistemas de información existentes, especificando las exigencias de seguridad. (Punto 12.1.1 ISO27002:2008)

Ejemplo: El laboratorio decide instalar un nuevo software para la gestión de los clientes y la facturación a los mismos.
Control: Como paso previo a la adquisición de software, se deben definir los requisitos de seguridad mínimos que el software debe garantizar y probar que se cumplen.
Implementación: El laboratorio decide realizar un estudio de los requisitos que debe tener el software antes de comprarlo. Decide los campos mínimos que debe llevar, las funcionalidades que debe cumplir con respecto a las medidas de seguridad, debe de identificar a los usuarios y llevar un registro de accesos de dichos usuarios. El software que adquiera el laboratorio cubrirá todas las necesidades del mismo.

B. ACTUALIZACIONES DE SOFTWARE

Las actualizaciones del software de la organización deben ser objeto de un tratamiento específico, que incluya la definición de un entorno de pruebas, en el que se valide que las actualizaciones permiten la ejecución de todas las aplicaciones inmersas en el entorno de producción. Establecer cauces de recepción de los parches o actualizaciones por parte de los fabricantes, su revisión y prueba y la puesta en producción de una forma eficaz, garantiza que

se minimiza la probabilidad de ser infectados por virus o software dañino que utilice defectos en el software[40].

- **Implantación de Medidas**

Se debe definir un procedimiento de actualización del software instalado en la empresa, estableciendo el cauce de recepción de parches y actualizaciones, normas para la realización de pruebas y traspaso de las actualizaciones al entorno de producción.

- **Normativa**

La implantación de normas y procedimientos para las actualizaciones de software está reflejada en la norma ISO 27002 en los siguientes puntos:

- La puesta en práctica de cambios deberá estar controlada mediante el empleo de procedimientos de control de cambios formales. (Punto 12.5.1 ISO27002:2008)

- Cuando se realizan cambios y/o actualizaciones en sistemas de información cruciales para la organización, éstos se deberán probar previamente para asegurar que no hay ningún impacto adverso sobre operaciones de organización o su seguridad. (Punto 12.5.2 ISO27002:2008)

Ejemplo: El laboratorio recibe semestralmente una actualización de su software de gestión de empresa.
Control: Se debe definir un procedimiento de actualización de parches y de equipos, asegurando que dichas actualizaciones se han probado previamente a su puesta en producción.
Implementación: El laboratorio, según su política de actualización, la instala en un equipo de pruebas fuera del sistema de información principal, con una base de datos de prueba, detectando las posibles anomalías antes de la implantación en todo el sistema de información.

[40] [4] IBID p 13.

C. PROTECCIÓN CONTRA CÓDIGO MALICIOSO

Los errores generados en el software instalado en la aplicación, pueden ser aprovechados por software malicioso para producir daños en el sistema, este hecho amenaza la integridad y la confidencialidad de los datos y debe ser gestionado adecuadamente. Los virus informáticos son aplicaciones o trozos de código que aprovechan estos errores.

- **Implantación de Medidas**

Se debe establecer una política de protección del sistema de información que incluya la instalación en todos los equipos de un software antivirus. Se deben adoptar medidas de seguridad complementarias a la instalación de un antivirus, como son establecer una planificación de actualizaciones del mismo, formar y concienciar al personal para que eviten la ejecución de archivos o lectura de mensajes no reconocidos, recomendando la eliminación de los mismos. También se debe contemplar en las medidas la prohibición de instalación de software sin licencia, ya que dicho software podría encubrir al software malicioso (virus, troyanos, etc.), así como el uso de software no autorizado específicamente por la organización[41].

- **Normativa**

La implantación de normas de protección contra código malicioso está reflejada en la norma ISO 27002 en el siguiente punto:

- Se deberán poner en marcha medidas para la detección, prevención y recuperación del sistema frente a código malicioso, así como procedimientos de concienciación de los usuarios. (Punto 10.4 ISO27002:2008)

Ejemplo: Los usuarios utilizan CD's y USB de fuera del laboratorio en los equipos del sistema de información de la empresa.

[41] [4] IBID p 13.

Control: Se debe definir un procedimiento de instalación y actualización de antivirus en la organización, desarrollando actuaciones de formación y concienciación complementarias a usuarios, para evitar la entrada de código malicioso en el sistema.
Implementación: El laboratorio decide instalar en todos los equipos un antivirus y mantenerlo actualizado, y establece normas para que cualquier soporte que se utilice (que no pertenezca a la empresa) primero se escanee con dicho antivirus. También establece normas para que solo el software legal y autorizado por el laboratorio sea instalado en los equipos del sistema de información.

D. COPIAS DE SEGURIDAD

En la actualidad, las organizaciones experimentan un continuo incremento de la cantidad de datos que necesitan para su funcionamiento, los datos automatizados pueden considerarse como críticos para la continuidad del negocio y deben estar expuestos al menor riesgo posible de pérdida, alteración o acceso no autorizado. Una estrategia de copias de seguridad adecuada, es el seguro más efectivo contra posibles desastres que puedan afectar al sistema de información de la organización, tales como incendios, inundaciones, fallos hardware, errores humanos, robos, virus, etc.

- **Implantación de Medidas**

Se deben establecer procedimientos para la gestión de copias de seguridad, que permitan recuperar la totalidad de los datos y configuración de los sistemas al instante anterior a la pérdida de datos. En función de la criticidad de los datos y del tiempo máximo para efectuar la recuperación, existen diferentes estrategias de copias de seguridad: cd, dvd, disco duro, dispositivos usb, etc. Estas son opciones a considerar antes de definir la política de copias. Las copias de seguridad tendrán que estar incluidas en el inventario de soportes, controlados sus movimientos entre la organización y el exterior, y garantizada su confidencialidad, reduciendo su manipulación y acceso exclusivamente a personal autorizado[42].

[42] [4] IBID p 13.

- **Normativa**

La implantación de procedimientos de realización de copias de seguridad está reflejada en la norma ISO 27002 en el siguiente punto:

- Las copias de respaldo de información y software deberían ser realizadas y probadas con regularidad, conforme a la política de seguridad y de continuidad de negocio. (Punto 10.5 ISO27002:2008)

Ejemplo: El laboratorio decide no realizar copias de seguridad y pierde la información de los clientes.
Control: Se debe establecer una política de copias de seguridad que garanticen la reconstrucción de los datos y configuración de los sistemas al instante anterior a la pérdida de información.
Implementación: El laboratorio decide establecer mecanismos de realización de copias de seguridad diarias, enviando fuera de las instalaciones una de las copias una vez a la semana. De esta forma, la empresa asegura la recuperación de los datos en caso de desastre hasta la última copia de seguridad realizada.

6.3.3.3.4 SEGURIDAD LÓGICA EN LAS COMUNICACIONES [43]

Es de vital importancia mantener el seguro acceso a los servicios de la red, tanto de manera interna como externa, controlando con políticas y restricciones para la capacidad de los usuarios con el fin de garantizar la protección de la seguridad de la información.

A. SEGURIDAD EN EL ACCESO A TRAVÉS DE REDES. IDENTIFICACIÓN AUTOMÁTICA DE EQUIPOS

El acceso externo al sistema de información corporativo debe estar limitado, asegurando dicho acceso solamente al personal autorizado. Una medida que ayuda a garantizar este acceso es

[43] [22] IBID p 61.

exigir la identificación automática del equipo que accede, evitando así la conexión desde equipos no seguros, o equipos que no están autorizados por la organización.

- **Implantación de Medidas**

Para aquellos laboratorios que permiten accesos externos a su sistema de información, se deben establecer mecanismos para la identificación automática de los equipos al acceder al sistema de información, autenticando así las conexiones desde terminales determinados. Se debe también implantar algún sistema de protección física a los equipos, para proteger la seguridad de su identificador[44].

- **Normativa**

La implantación de mecanismos de identificación automática de equipos ante el sistema está recogida en la norma ISO 27002, en los siguientes puntos:

- La red debería estar suficientemente protegida para evitar amenazas tanto en los sistemas que la componen como en la información que transita por ella. (Punto 10.6.1 ISO27002:2008)

- Para redes compartidas, sobre todo aquellas que se extienden fuera de las fronteras de la organización, la capacidad de acceso de los usuarios a la red debería ser restringida, al igual que el acceso a las aplicaciones de gestión, poniendo en práctica los requisitos de seguridad establecidos. (Punto 11.4.6 ISO27002:2008)

- La identificación de equipo automática, deberá ser considerada como el medio de autenticar conexiones de posiciones específicas y equipos.(Punto 11.4.3 ISO27002:2008)

Ejemplo: El laboratorio dispone de accesos externos al sistema de información desde el exterior.
Control: Para aquellos laboratorios que permiten accesos externos a su sistema de

[44] [4] IBID p 13.

información se debe establecer un sistema de identificación automática de los equipos externos para garantizar que el acceso está autorizado.
Implementación: El laboratorio decide definir que los usuarios externos solo podrán conectarse desde unos equipos determinados, que garantizan los niveles de seguridad exigidos por la empresa. De esta forma evita que se pueda acceder al sistema de información desde terminales que no sean de confianza.

B. CIFRADO

En las ocasiones en que el nivel de seguridad legalmente establecido y/o la confidencialidad de los datos así lo requieran, se debe implantar en el sistema de información de la organización el uso de sistemas y técnicas criptográficas, siempre que otras medidas y controles no proporcionen la protección adecuada o requerida. El cifrado es una técnica para proteger la confidencialidad de la información clasificada de la organización que pueda verse comprometida.

- **Implantación de Medidas**

En las ocasiones en que el nivel de seguridad legalmente establecido y/o la confidencialidad de los datos así lo requieran, se debe implantar en el sistema de información de la organización el uso de sistemas y técnicas criptográficas, cuando otras medidas y controles no proporcionen la protección adecuada o requerida. Para ello, se deben establecer procedimientos y mecanismos que contemplen los casos en el que la información debe cifrarse, y los mecanismos a utilizar para dicho cifrado[45].

- **Normativa**

La implantación de normas y mecanismos de cifrado está reflejada en la norma ISO 27002 en los siguientes puntos:

[45] [4] IBID p 13.

- Una política de empleo de controles criptográficos para la protección de información debería ser desarrollada y puesta en práctica. (Punto 12.3.1 ISO27002:2008)

- Los controles criptográficos deberían ser usados desde el cumplimiento con todos los acuerdos relevantes, leyes y regulaciones. (Punto 15.1.6 ISO27002:2008)

Control: Para el tratamiento de datos de carácter personal, especialmente protegidos, o que para la organización sean confidenciales, se debe definir un procedimiento de cifrado de la información que garantice la confidencialidad de los datos.

6.3.3.4 CONTROLES RELACIONADOS CON LA REVISIÓN DEL SISTEMA[46]

En este apartado se relatan las medidas de seguridad que se deben aplicar al sistema de información para permitir una adecuada revisión de los sistemas y medidas implantadas, y para establecer registros fiables que recojan pruebas de auditoría para evaluar el cumplimiento de las medidas de seguridad.

A. CONTROL DE REGISTRO DE ACCESO

La correcta configuración de los registros de acceso a los sistemas, detecta el intento de intrusión de personal externo a la organización, o de personal interno que intenta acceder a recursos a los que no está autorizado. Es importante una correcta configuración de los registros de acceso y una periódica revisión de dichos registros para detectar incidencias de seguridad que pueden ser corregidas.

- **Implantación de Medidas**

Se deben configurar procedimientos y registros de control de acceso, para validar que los usuarios que acceden a los recursos están autorizados y almacenar evidencias de cualquier

[46] [22] IBID p 61.

intento de acceso no autorizado. Los registros de acceso deben estar protegidos ante manipulaciones o alteraciones[47].

- **Normativa**

La implantación de controles para los registros de acceso está reflejada en la ISO 27002, en los siguientes puntos:

- Los errores de acceso deberán ser registrados, analizados y servir como soporte para llevar a cabo acciones correctivas. (Punto 10.10.5 ISO27002:2008)
- Las actividades de auditoria y verificación de sistemas operacionales deberán ser planificadas para evitar interrupciones en los procesos de negocio. (Punto 15.3.1 ISO27002:2008)
- Los registros de las instalaciones y la información de los logs deberán estar protegidos contra el acceso no autorizado. (Punto 10.10.3 ISO27002:2008)

Control: Se deben configurar registros de acceso que contengan la identificación de los accesos al sistema.

B. SINCRONIZACIÓN DE RELOJES

La correcta sincronización de relojes de los procesadores es esencial para la exactitud de los datos reflejados en los archivos de registro (log's) y para la realización de auditorías, investigación de incidencias, o como prueba en casos legales o disciplinarios. La inexactitud de los registros de auditoria puede inutilizar las evidencias recogidas.

- **Implantación de Medidas**

Todos los relojes de los equipos del sistema de información se deberían sincronizar ajustado a la norma acordada UTC (Tiempo Universal Coordinado) y ajustado a la hora local

[47] [4] IBID p 13.

normalizada. Este hecho permite la correcta realización de un análisis del rastro dejado por una evidencia en la secuencia de acciones cronológicamente correcta en el tiempo[48].

- **Normativa**

La implantación de mecanismos de sincronización de relojes está reflejada en la ISO 27002 en el siguiente punto:

- Los relojes de todos los sistemas de informática relevantes de tratamiento de información o de dominio de seguridad, deberán ser sincronizados con una fuente de tiempo reconocida y exacta. (Punto 10.10.6 ISO27002:2008)

Ejemplo: El laboratorio sufre una pérdida de información en su sistema, y quiere analizar por qué, ya que no ha tenido ningún problema físico ni lógico que se conozca.
Control: Sincronizar los relojes de los servidores con arreglo a la norma UCT (Tiempo universal Coordinado).
Implementación: El laboratorio definió todos los equipos para que sincronizaran la hora desde el servidor, con lo que le permite comprobar qué equipos estaban conectados en el sistema de información, y al mirar los registros de dichos equipos, puede llegar a una conclusión sobre lo ocurrido.

[48] [4] IBID p 13.

6.3.4 FORMACIÓN, TOMA DE CONCIENCIA Y COMPETENCIA.

Como último paso en el HACER, la norma ISO 27001 establece que la organización debe asegurar que todo el personal que tenga responsabilidades con el SGSI debe ser competente para cumplir sus tareas. Para garantizar sus competencias el laboratorio debe determinar las competencias necesarias de los colaboradores, realizar actividades de formación o contratar personal si es necesario, evaluar la eficacia de las acciones que se están realizando y mantener registros de las formaciones, habilidades, experiencia y calificaciones. El laboratorio debe asegurar que todos los colaboradores tomen conciencia de la pertinencia e importancia de sus actividades de seguridad de la información y su influencia en el cumplimiento de los objetivos del SGSI[49].

6.3.5 OBJETIVOS DE CONTROL E INDICADORES.

La Norma estipula que se deben incluir las acciones que se van a realizar para gestionar el riesgo en el plan de tratamiento. Estas acciones serán parte de la mejora continua del SGSI y se debe medir, estableciendo objetivos e identificando las oportunidades de mejora. Una vez establecidos los objetivos, se debe establecer los indicadores de rendimiento para medir el cumplimiento de los objetivos. Para poder medir es necesaria la información que se recogerá a partir de los registros del sistema reflejados en cada uno de los documentos, para realizar una medición adecuada la información debe ser pertinente, precisa y oportuna[50].

Para proceder a construir el indicador se establecen las variables que lo conforman y la relación entre ellas para que se genere la información necesaria. Las variables se deben definir con la mayor rigurosidad posible asignándole un sentido claro, para evitar que se originen ambigüedades y discusiones sobre sus resultados. Así mismo, se debe tener claridad de quien y como produce dicha información para de esta forma mejorar el criterio de confiabilidad.

[49] [4] IBID p 13.
[50] [4] IBID p 13.

Es importante realizar un control del indicador para determinar si es adecuado para la información que se quiere obtener. Si no cumple con los criterios de selección es necesario definir nuevos indicadores[51].

Tabla 1. Criterios para selección de indicadores

Criterio de selección	Pregunta a tener en cuenta	Objetivo
Pertinencia	¿El indicador expresa qué se quiere medir de forma clara y precisa?	Busca que el indicador permita describir la situación o fenómeno determinado, objeto de la acción.
Funcionalidad	¿El indicador es monitoreable?	Verifica que el indicador sea medible, operable y sensible a los cambios registrados en la situación inicial
Disponibilidad	¿La información del indicador está disponible?	Los indicadores deben ser construidos a partir de variables sobre las cuales exista información estadística de tal manera que puedan ser consultados cuando sea necesario.
Confiabilidad	¿De donde provienen los datos?	Los datos deben ser medidos siempre bajo ciertos estándares y la información requerida debe poseer atributos de calidad estadística.
Utilidad	¿El indicador es relevante con lo que se quiere medir?	Que los resultados y análisis permitan tomar decisiones.

Fuente: Metodología línea base de indicadores, DANE 2009

Aparte de generar indicadores para los objetivos se pueden establecer métricas en cuanto a cualquier parámetro relevante, por ejemplo la disponibilidad o la confidencialidad. Los valores de los parámetros que componen los objetivos (indicadores y métricas) tienen que recogerse de manera objetiva y regularmente para poder evaluar el progreso apropiadamente, por ejemplo:

- Objetivo: Aumentar un 20% la disponibilidad del sistema.

[51] Metodología línea base de indicadores. DANE 2009.

- Indicador: % de disponibilidad de los sistemas.
- Métricas: Nº de horas de parada del sistema/ Nº de horas de funcionamiento.

Los valores recogidos se van comparando en el tiempo con los objetivos marcados, para analizar las diferencias con los mismos y tomar las medidas oportunas cuando no se alcanzan. Esto con el fin de mejorar el proceso de toma de decisiones. Adicionalmente los indicadores permitirán cuantificar los cambios, monitorear el cumplimiento de los requisitos del SGSI, efectuar seguimiento a los planes que permita tomar las acciones correctivas oportunas y mejorar la eficiencia y eficacia del proceso en general.

6.4 VERIFICAR

Una vez que está en marcha el SGSI es fundamental hacer un seguimiento de cómo funciona y cómo va evolucionando el sistema. En primer lugar para corregir las posibles desviaciones sobre lo planificado y previsto y en segundo lugar, aunque igual de importante, detectar oportunidades de mejora del sistema, ya que el objetivo último de implantar un sistema de gestión de este tipo es el mejorar continuamente, hacer cada vez más con los limitados recursos disponibles.

6.4.1 REVISIÓN DEL SGSI

Uno de los requisitos más relevantes de la Norma ISO 27001 es la revisión que la dirección de la organización debe realizar con una cierta periodicidad, como mínimo anual, al Sistema de Gestión de Seguridad de la Información. Esta revisión tiene como objetivo asegurarse de que el SGSI es en todo momento adecuado, apropiado y efectivo para los propósitos y contexto de la organización. Esta revisión forma parte de la fase VERIFICAR del ciclo de mejora continua, y es una herramienta magnífica para el análisis y la adopción de oportunidades de mejora, ya que se contemplan todos los aspectos y la marcha del SGSI, por lo que se tiene una visión general de todo y se pueden detectar los puntos débiles y discutir sobre cómo mejorarlos. Existen muchas formas en que la alta dirección puede revisar el SGSI como, por ejemplo, recibir y revisar un informe generado por el representante de la dirección u otro personal, o incluir los temas pertinentes en la agenda de reuniones regulares de la dirección[52].

Entradas para el proceso:

Existen muchas fuentes de las que se pueden recoger datos e información útiles para realizar la revisión por la dirección:

Las auditorías llevadas a cabo en la organización. No sólo las auditorías internas del SGSI son útiles aquí, sino también otras auditorías tales como auditorías de clientes, de otras normas de gestión, etc. Todas ellas pueden aportar información sobre los puntos fuertes y débiles del SGSI y poner en evidencia oportunidades de mejora.

[52] [4] IBID p 13.

Las anteriores revisiones del SGSI y las acciones derivadas del mismo, son el punto de partida, dónde estaba el SGSI y qué es lo que se ha hecho al respecto desde entonces. Analizar qué se decidió hacer y hasta donde se ha avanzado, proporciona información muy valiosa sobre qué se puede hacer para continuar mejorando y progresando. Estudiar por qué no se han llevado a cabo todas las acciones planificadas servirá para detectar puntos débiles y obliga a determinar nuevas medidas.

Comentarios de las partes interesadas. A lo largo de la actividad cotidiana de la organización, tanto clientes, como usuarios, proveedores, público, cualquiera que entra en contacto con ella puede emitir algún comentario que puede ser útil para diseñar alguna acción de mejora. Debe existir algún mecanismo, aunque sea informal para incorporar esta información al sistema.

Técnicas, productos o procedimientos, que podrían ser usados en la organización para mejorar el funcionamiento y la efectividad del SGSI. La información necesaria para este punto probablemente vendrá en primer lugar del responsable de sistemas, pero también las distintas personas involucradas en tareas que necesiten mejoras pueden aportar ideas al respecto.

El estado de las acciones preventivas y correctoras. Hay que analizar las acciones, que son la medida de cómo se desarrolla la actividad cotidiana del SGSI, estudiando cuantas se han abierto, por qué motivo, si se han ido cerrando en plazo, si ha habido problemas con alguna de ellas, etc. Con esa información se extraerán conclusiones importantes para la mejora del SGSI.

Las vulnerabilidades o amenazas que no se han tratado adecuadamente en análisis de riesgos anteriores. Es decir, si se han detectado nuevas amenazas o ha habido cambios que necesiten revisar las anteriormente consideradas, o bien valorar si riesgos que no se trataron por cualquier motivo antes, ahora necesitan de tratamiento.

La evaluación de los objetivos. Uno de los principales puntos de esta revisión es comprobar si se han conseguido los objetivos marcados en un principio. Cuando se diseña el SGSI, se marcan unos objetivos, para los que habrá que definir unas métricas que permitan evaluar hasta qué punto se han alcanzado los objetivos. Esta información es la que indica si el SGSI funciona o no, si es eficaz o no. A la luz de esta información se podrá decidir si hay que modificar los objetivos o qué acciones tomar para alcanzarlos.

Cambios en la organización. Cambios por ejemplo en la infraestructura informática por ejemplo, que afectaría de manera directa y clara al SGSI, ya que las medidas de seguridad aplicadas en los anteriores sistemas de información pueden no ser válidas o suficientes para los nuevos sistemas. Pero también cambios en el personal, que requieran reajustar los privilegios en el acceso a la información, en los servicios que la organización ofrece, que pueden plantear nuevos requisitos de seguridad, etc.

Salidas del proceso:

Mejoras de la efectividad del SGSI, es decir, qué se va a hacer para mejorar el SGSI: se van a implantar más controles, se van a mejorar los ya implantados, se van a transferir riesgos, etc.

Actualización de la evaluación y gestión de riesgos. Hay que documentar los cambios que se hayan producido en el análisis y gestión de los riesgos y los motivos que los han motivado.

Modificación de procedimientos y controles que afectan a la seguridad de la información, según sea necesario, para responder a incidentes internos o externos que puedan impactar en el SGSI, incluyendo cambios en:

Requisitos de negocio, de seguridad o legales.

Procesos de negocio que tengan efecto en los requisitos de negocio existentes.

Obligaciones contractuales.

Cambios en el nivel de riesgo aceptable.

Necesidades de recursos.

Mejoras en la manera de medir la efectividad de los controles. Al revisar los indicadores que se utilizan debe comprobarse si siguen siendo útiles, eliminando aquellos que no lo sean y diseñando nuevos indicadores más eficaces a la hora de suministrar información relevante.

6.4.2 HERRAMIENTAS PROPUESTAS

En la etapa del verificar es viable implementar herramientas como cartas de control, planes de verificación del SGSI, balanced scorecard o cuadro de mando integral y el programa de auditorías internas, entre otros, que faciliten realizar el seguimiento del SGSI y determinar su cumplimiento de acuerdo a la ISO 27001. (Ver anexo 5)

La metodología propuesta se aplica al laboratorio de análisis microbiológico en esta etapa del verificar teniendo en cuenta su contextualización en el planear y hacer. A partir de la matriz AMFE desarrollada para el proceso de "Elaboración de informe de resultados" se definió la prioridad de los riesgos de acuerdo al IPR calculado en el análisis de la gravedad, frecuencia y detectabilidad de los riesgos presentes o potenciales en cada activo de información.

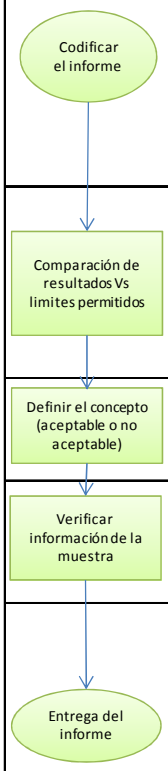
El resultado de la matriz AMFE evidencia que en el proceso descrito se debe dar prioridad a trece (13) riesgos, es decir aquellos que obtuvieron un IPR mayor o igual a 15 son los riesgos que deben ser controlados por el SGSI.

Para verificar el cumplimiento de los métodos de control establecidos por el SGSI del ejemplo del laboratorio, se desarrolló el plan de verificación del SGSI (tabla 9) propuesto como una herramienta para cinco de los riesgos (5) de mayor prioridad. En el cual se evidencia un consolidado del proceso, métodos de control y resultado de los indicadores. En este caso no se cumple la meta de dos indicadores que corresponden a los riesgos:

- Dar un concepto errado al resultado de la muestra
- Asignar la información equivocada de la muestra (lote, fechas, etc)

De una manera práctica el Plan de verificación permite identificar los riesgos que no se están tratando correctamente en el SGSI por múltiples causas o variables, al conocer el consolidado de los indicadores. Por lo tanto brinda la información para tomar decisiones y determinar las acciones preventivas o correctivas correspondientes (Actuar). Además de ser una herramienta para evaluar periódicamente los procesos y controlar la residualidad de los riesgos al determinar si los métodos de control no son eficientes y eficaces.

Tabla 9 Plan de verificación del SGSI Fuente: Los autores

LOGO DE LA ORGANIZACIÓN	PLAN DE VERIFICACIÓN DEL SGSI							
	ALCANCE: Este plan de verificación aplica para el proceso misional Elaboración de informe de resultados. Desde su codificación hasta la entrega del informe al cliente.							
	OBJETIVOS DEL SGSI: Verificar el cumplimiento de los metodos de control establecidos para los riesgos de este proceso.							
Nombre del proceso	**Diagrama de flujo del proceso**	**Procedimiento**	**Riesgo a controlar**	**Metodo de control de proceso**			**Objetivo de control**	**Indicador**
				Control implementado	**Registro**	**Responsable**		
ELABORACIÓN DE INFORME DE RESULTADOS		POE08	Mal funcionamiento del servidor	Realizar actividades de mantenimiento preventivo del servidor y conectividad.	Orden de servicio del área de sistemas y soporte	Coordinador del SGSI	Se deben establecer procedimientos de mantenimiento del servidor de forma periódica.	Porcentaje de cumplimiento: 97%. Meta: 95%
		POE10	Ajuste de resultados por conveniencia	Se limita el acceso al software del laboratorio de acuerdo al rol del personal . Se registran los cambios de datos y autorizaciones.	Base de datos control de cambios en el servidor. Se registra el usuario que autoriza.	Coordinador del SGSI	Definir las funciones y responsabilidades (roles) de todo el personal formalmente.	Porcentaje de cumplimiento: 100%. Meta: 100%
		POE10	Dar un concepto errado al resultado de la muestra	Realizar una revisión técnica del informe y dar la aprobación.	Registro de aprobación en el software	Director técnico	Asegurar la revisión técnica del documento y su aprobación.	Porcentaje de cumplimiento: 90%. Meta: 95%
		POE10	Asignar la información equivocada de la muestra (lote, fechas, etc)	Realizar una revisión técnica del informe y dar la aprobación.	Registro de aprobación en el software	Director técnico	Asegurar la revisión técnica del documento y su aprobación.	Porcentaje de cumplimiento: 88%. Meta: 95%
		POE10	Perdida de información	Diariamente configurar el servidor para realizar backup de la información y el coordinador debe hacer backup manual en un dispositivo movil restringido.	Registro del backup, fecha y hora.	Coordinador del SGSI y calidad	Realizar copias de seguridad de la información.	Porcentaje de cumplimiento: 98%. Meta: 95%
AUDITORIA: Se realizarán mensualmente, con el proposito de evaluar de manera objetiva el seguimiento y eficacia del plan y verificar la conformidad de los requisitos especificados. **Elaborado por: LIDER DE CALIDAD Y COORDINADOR SGSI Fecha de emisión: 02/07/2012**								

6.4.3 AUDITORIAS INTERNAS

Podemos definir auditoría como una actividad independiente que tiene lugar dentro de la organización y que está encaminada a la revisión de operaciones con la finalidad de prestar un servicio a la dirección, ya que en realidad es un control de dirección El objetivo de una auditoría es determinar si los objetivos de los controles, los controles, los procesos y los

procedimientos están conformes con los requisitos de la Norma en la que se audite el sistema, los requisitos legales y reglamentarios, los requisitos de la organización (contractuales, de seguridad, internos, etc.). Además de esto, la auditoría verifica si el SGSI se mantiene de manera efectiva y se obtienen los resultados esperados. Es decir, si el sistema dice lo que hace y hace lo que dice. La planificación de la auditoría debe hacerse al menos anualmente, ya que es importante realizar una revisión al sistema completo a lo largo del año, decidiendo no solo las fechas en las que se va a realizar, sino si el alcance va a ser global o parcial y en este último caso, las áreas y procesos que van a ser auditados en cada una de las auditorías. Una vez hecho esto, se puede comenzar a preparar la auditoría en sí, decidir los criterios de auditoría, el método que se va a utilizar e informar a los afectados por la auditoría con tiempo suficiente para que se puedan preparar. Los auditores designados para la realización de la auditoría prepararán una lista de comprobación que incluirá datos como el alcance de la auditoría, las actividades a auditar, los documentos aplicables tales como las normas aplicables y la política de seguridad, documentos de referencia como los informes de otras auditorías o la revisión del sistema, además de la fecha prevista de realización. Esta lista será la guía de trabajo para la ejecución de la auditoría, que revisará las actividades y las evidencias de que se realizan según los requisitos y los controles aplicables. Una vez hechas las comprobaciones, se redacta y entrega a dirección y a los afectados el informe de resultados, identificando las no conformidades detectadas, es decir, las desviaciones o los incumplimientos de la Norma de referencia de la auditoría o de las normas internas de la organización. Con esta información se deben tomar las medidas oportunas para solucionarlas, identificando las causas de las no conformidades y eliminándolas. El objetivo siempre será detectar problemas con los procesos y procedimientos nunca con el personal encargado de ejecutarlos, para poder mejorar continuamente[53].

Las personas que asuman el rol de auditor Interno tienen que poseer la necesaria preparación profesional en las metodologías que hay que emplear, los conocimientos generales (tanto del ambiente empresarial como del SGSI) y contar con el carisma personal para tener credibilidad y el respaldo de la dirección. Es muy importante que sean personas que tengan independencia en relación con las actividades involucradas. Los resultados de una auditoría realizada por

[53] Implantación de un sistema de gestión de la seguridad de la información y certificación ISO 27001 en la Administración Pública. Tecnimap 2010.

alguien que realiza o controla el trabajo auditado estarán probablemente sesgados, por lo que debe evitarse esta situación.

El proceso de auditoría según la ISO 19011 consiste en:

- Programa de auditoría: conjunto de una o más auditorias planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico. Incluye las actividades para planificar y organizar el número de auditorías, los recursos y el tiempo.
- Realizar el plan de auditoría: Este documento incluye, el objetivo, el alcance, criterios, fechas, hora de cada actividad, recursos y equipo auditor seleccionado. En esta etapa se ejecuta el plan para determinar el cumplimiento de los requisitos de la ISO 27001 los cuales pueden estar documentados en una lista de chequeo de manera práctica para los auditores.

Las actividades in situ son:

- Realización de la reunión de apertura. Es importante este espacio para dar claridad al objetivo, alcance y criterios de la auditoria.
- Comunicación durante la auditoria
- Recopilación y verificación de la información
- Generación de hallazgos de la auditoria
- Realización de la reunión de cierre. Es importante este espacio para dar a conocer a la gerencia y dueños de proceso las fortalezas, observaciones y oportunidades de mejora del SGSI, para aprobar el informe de auditoría.
- Seguimiento y revisión del programa: Se identifican acciones preventivas y correctivas y oportunidades de mejora del sistema de seguridad de la información.
- Se establece la mejora del programa de auditoría.

6.5 ACTUAR

La implantación del SGSI debe ser un proceso dinámico, para esta etapa debe estar claro que la misión del SGSI es situar la seguridad de la información al mismo nivel que cualquier otro objetivo de negocio, y como tal, debe ser optimizado continuamente. Esta etapa corresponde al Capítulo 8 de la ISO 27002. Es en esta fase cuando deberemos implantar las medidas correctivas fruto de las revisiones efectuadas, y mejorar así el rendimiento del SGSI. Las medidas correctivas comprenden la selección de nuevos controles, la modificación de los existentes o la eliminación de los obsoletos. Resulta bastante frecuente que se haga necesario rectificar el alcance inicial del SGSI y su diseño[54].

Es así que en esta etapa deberá tenerse en cuenta:

1. Identificar no conformidades del SGSI.
2. Realizar análisis de causa raíz
3. Definir acciones correctivas y preventivas.
4. Identificar las mejoras potenciales del SGSI que se hayan propuesto en la fase anterior y ponerlas en marcha.
5. De ser necesario, obtener el visto bueno de la Dirección para la implementación de los cambios propuestos y aprobación de recursos necesarios
6. Divulgar o comunicar las acciones y mejoras a todos los interesados.
7. Evaluar la efectividad del plan de mejora continua tomando como base los resultados obtenidos de las acciones implementadas y realizar planes de acción concretos para mejorar el SGSI.

[54] [4] IBID p 13.

Entradas para el proceso:

1. Informes de Auditoría interna.
2. Informes de no conformidades.
3. Informes de conclusiones y sugerencias que surjan de la etapa de revisión.
4. Propuestas de mejoras de otras áreas y unidades de negocios.

Personas responsables

1. Equipo de Planeamiento de la Seguridad de la información, responsable de sugerir las mejoras que pueden obtenerse y estimar los recursos que serían necesarios.
2. Alta Gerencia en caso de ser los cambios propuestos de un impacto considerable o requerir presupuesto adicional al ya otorgado.

Salida del proceso:

Un Informe con el plan de mejoras, describiendo o referenciando las conclusiones más relevantes surgidas de la etapa de revisión y especificando objetivos concretos, el impacto de los cambios y quienes estarían involucrados así como un plan tentativo para llevarlos a cabo. Los planes de mejoras deberán ser coordinados, de forma de interferir lo menos posible en la operativa diaria del laboratorio para evitar interferencias en los procesos.

6.5.1 HERRAMIENTAS PROPUESTAS

Existen diversas herramientas que se han desarrollado con el fin de ayudar a establecer planes de acción efectivos al momento de resolver un problema dentro de una organización, en el Anexo 6, se muestran algunas herramientas fáciles de aplicar en el sector de laboratorios

A continuación se desarrollan, a manera de ejemplo, los pasos propuestos en la fase del Actuar, haciendo uso de algunas de las herramientas propuestas en el Anexo 6.

1. Identificar no conformidades del SGSI.

   Con base en la revisión de resultados del sistema, se ha detectado una no conformidad por el incumplimiento del objetivo trazado para el proceso *Elaboración de informe de resultados* en la operación *definir el concepto del análisis de la muestra*, tal como el Plan de Verificación de SGSI (ver tabla 9.) el indicador tiene una meta del 95% y el resultado del periodo fue del 90% de cumplimiento.

   Adicional existe otra no conformidad en la operación *verificar información de la muestra* del mismo proceso, con un resultado del 88% cuando la meta es del 95%. Tomaremos la operación de *definir el concepto del análisis de la muestra* para el desarrollo de los siguientes puntos.

2. Realizar análisis de causa raíz

   Para detectar la causa raíz de la generación de conceptos errados del análisis de la muestra utilizaremos la metodología de los 5 ¿Por qué?

   Situación detectada: en la revisión técnica del informe previa a la publicación se han detectado que el 10% de los conceptos finales han sido errados.

   ¿Por qué están errados los conceptos?

   Porque el concepto que emiten los analistas no coinciden con el del director técnico, que en la revisión del informe, comparar los resultados con el estándar o patrón de análisis.

   ¿Por qué no coinciden los conceptos emitidos por los analistas con los emitidos por el director técnico?

   Porque se detecto que no están utilizando los mismo estándares o patrones de análisis.

   ¿Por qué los analistas y el director técnico no están usando los mismos patrones para el análisis y generación del concepto final de la muestra?

   Porque el director técnico, quien se encarga de actualizar el servidor de la compañía desde su computador personal cargando la base de datos de los patrones de

comparación para los análisis, tiene siempre información de primera mano actualizada, los analistas trabajan muchas veces con patrones desactualizados que están en el servidor de la compañía, en la ruta indicada.

¿Por qué la información del servidor, en la ruta indicada para consultar los patrones para comparación de muestras no se encuentra actualizada, si el director técnico actualiza permanentemente dicha información desde su computador personal?

Porque la actualización del servidor se corre semanalmente todos los viernes después de las 6 pm.

¿Por qué la actualización de la información en el servidor se corre semanalmente?

Porque no se cuenta con un servidor lo suficientemente robusto, que permita tener información actualizada a toda la compañía en tiempo real.

Finalmente se ha llegado a la causa raíz del problema, el servidor no tiene la capacidad para actualizar en tiempo real la información que carga el director técnico desde su computadora.

3. Definir acciones correctivas y preventivas.

Acciones correctivas.

a. El Director Técnico, en el momento en que actualiza información de patrones de comparación al servidor, enviara vía e-mail a todos los analistas dicho archivo, notificándoles el cambio de versión del documento.

b. Los analistas deberán verificar cada vez que les llegue el e-mail de actualización de información por parte del Director Técnico, que sea la misma que se encuentra en el servidor en la ruta indicada, de lo contrario deberán trabajar con la información enviada por el Director.

Acciones preventivas.

a. Conseguir un servidor que permita información actualizada en tiempo real.

4. Identificar las mejoras potenciales del SGSI que se hayan propuesto en la fase anterior y ponerlas en marcha.

   Para realizar este análisis se recomienda tener en cuenta el costo-beneficio de las acciones planteadas, la mejor opción será la que genere un mayor impacto en el proceso con un retorno de inversión más corto.

Los pasos 5, 6 y 7 se deben llevan a cabo obligatoriamente en la práctica del ejercicio.

6.5.2 ACCIONES CORRECTIVAS Y PREVENTIVAS

Cuando se producen no conformidades, es decir, cuando hay un incumplimiento de un requisito, bien de la Norma bien de las pautas internas, se deben toman acciones encaminadas a resolver esa situación no deseada. Las acciones contempladas por la Norma se dividen en:

Acciones correctivas.

Acciones preventivas.

Acciones de mejora.

Las acciones correctivas son las que se toman para corregir una no-conformidad significativa con los requisitos del Sistema de Gestión de Seguridad de la Información. Se pueden detectar no conformidades durante cualquiera de las auditorías y revisiones a las que se somete el SGSI, al analizar los registros de incidencias, ya las que sean graves o reiteradas en el tiempo constituyen no conformidades, o durante la operativa habitual del SGSI. Localizado un problema debe determinarse la relación causa-efecto para determinar el curso de acción. Las acciones correctivas tienen como objetivo la eliminación de la causa origen del problema para evitar que éste se pueda repetir en el futuro. Solucionar momentáneamente el incidente no es una acción correctiva completa. Evidente es necesario restablecer el servicio u operación que se haya visto afectada por el incidente, pero debe descubrirse el por qué del mismo[55].

[55] [4] IBID p 13.

Las acciones preventivas como su propio nombre indica, son aquellas que se toman para eliminar la causa de una posible no conformidad, es decir, se actúa antes de que ocurra. En una acción preventiva se determina la posible fuente de problemas antes de se haya materializado, con el objeto de eliminarla y evitar que se produzca. Como fuentes de información para el establecimiento de acciones preventivas son, entre otras, los resultados de las auditorías internas y externas, los resultados de los análisis de datos, los registros de gestión, el personal, las mediciones y métricas, etc. Habitualmente tanto las acciones correctivas como las preventivas se discuten y analizan, dentro del Comité de Seguridad. En ambos casos, para abrir una acción es necesario recoger todos los datos e información relativos al problema a tratar. A partir de ahí se trata de determinar el origen del problema y las primeras acciones a tomar, los responsables de ejecutar estas acciones y los plazos para ello. Se hace un seguimiento de la acción hasta que se hayan completado todas las acciones planificadas. Para cerrar una acción debe verificarse que se ha resuelto satisfactoriamente, es decir que ha sido efectiva.

Cuando se deciden acciones que no están relacionadas con una no conformidad éstas se denominan acciones de mejora. Pueden venir de sugerencias del personal, de la revisión del SGSI, etc. Estas acciones suponen un cambio positivo en la manera de afrontar una tarea o procesos de manera que se mejoren la operativa, los resultados o ambas. No se debe olvidar que el SGSI se basa en un ciclo de mejora continua por lo que es importante que en cada ciclo del proceso se sigan implantando medidas que mejoren el mismo.

6.6 DOCUMENTACIÓN DEL SGSI

Basados en la norma ISO 27001 se tendrá documentación desde nivel 1 hasta nivel 4 donde se incluyen el manual de seguridad, los procedimientos, los formularios y los registros. Adicional a esto se tendrán los documentos que enmarcan el SGSI y el control que se debe tener de los mismos[56].

[56] [4] IBID p 13.

- **Documentos de nivel 1**

Manual de seguridad: es el documento que inspira y enmarca el sistema, expone y especifica las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales. Es un análogo al manual de calidad.

- **Documentos de nivel 2**

Procedimientos: son la estandarización de los procesos operativos que aseguran el cumplimiento de la planificación, operación y control de los procesos de seguridad de la información de una forma eficaz.

- **Documentos de nivel 3**

Formularios: también conocidos como checklist o instrucciones los cuales describen las tareas y actividades específicas relacionadas con la seguridad de la información.

- **Documentos de nivel 4**

Registros: documentos que proporcionan evidencia del cumplimiento de los requisitos, están asociados a documentos de los otros niveles como elemento de salida que demuestra el cumplimiento de lo que se estipula en los mismos.

- **Documentos específicos del SGSI**

De manera específica ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos: Alcance del SGSI, Política y objetivos de seguridad, Procedimientos y mecanismos de control que soportan al SGSI, Enfoque e informe de evaluación de riesgos, Plan de tratamiento de riesgos y Declaración de aplicabilidad

- **Control de documentos**

Para todos los documentos que se generen en el SGSI se debe establecer, documentar, implementar y mantener un procedimiento que defina cuales es la gestión para: aprobar documentos, revisar y actualiza documentos, garantizar la identificación de los cambios y el estado actual de revisión de los documentos, la vigencia de los documentos y la disponibilidad para el lugar donde se utiliza, garantizar que los documentos se mantengan legibles y

fácilmente identificables, el control de la distribución de los documentos, prevenir el uso de los documentos obsoletos e identificar los documentos que son retenidos. Se deben establecer y mantener registros para brindar evidencia de la conformidad con los requisitos y la operación eficaz del SGSI.

7. CONCLUSIONES

- El establecimiento de un SGSI en una compañía es de gran utilidad al proporcionar una metodología adecuada para garantizar la confidencialidad, la integridad y la disponibilidad de los activos de su negocio que tengan que ver con la información.

- Tan importante como los procesos y procedimientos es el diseño de una organización que pueda desarrollar todas las actividades del negocio en la línea con lo indicado en el SGSI para lo cual es importante que la organización sea transversal y su enfoque sea por procesos.

- El SGSI diseñado ha de ser dinámico y fácilmente adaptable a los cambios y las mejoras a introducir en la compañía, la aplicación del modelo PHVA (Planear, Hacer, Verificar, Actuar) es fundamental, basado en el concepto de mejora continúa, la competencia en su manejo es de gran utilidad en contexto de un SGSI. El enfoque sistémico propuesto por la norma ISO/IEC 27001 permitirá las siguientes consecuencias:

- La toma de decisiones sobre la seguridad de los activos críticos de información se basa en información a priori (análisis de riesgos) y a posteriori (auditorías e indicadores).

- Se orienta a la mejora continua, a través de la gestión de acciones correctivas y preventivas.

- Si se decide obtener la certificación ISO/IEC 27001 del sistema, mejora la imagen del organismo y se contribuye a generar confianza entre los usuarios y la empresa.

- La importancia que para garantizar la seguridad de los activos de la información tiene desarrollar una gestión orientada a mitigar el impacto de los riesgos para lo cual se ha de diseñar un método de evaluación de riesgos completo que ha de permitir conocerlos y afrontarlos de forma coordinada, como lo hace el método de evaluación incluido en el trabajo. Y, seguidamente, definir unos planes bien de acción o bien de seguimiento con unos controles de seguridad que permitan verificar el rendimiento de cada plan.

- Es fundamental la concreción de los controles de seguridad para supervisar el seguimiento de los planes de acción, los controles incluidos, concretos y medibles en el tiempo permiten evaluar la efectividad de los planes de acción.

- Los objetivos son claramente el marco para definir los niveles de seguridad que se incluirán en el SGSI, para el sector de laboratorios donde la información es clave para mantener la continuidad del negocio es necesario trabajar en el diseño.

- El análisis del riesgo y la aplicación de los controles para su tratamiento incluye todos los procesos del laboratorio tanto misionales como gerenciales y de apoyo por lo que se necesitara implicación máxima de la dirección para llevar a cabo la metodología PHVA.

8. BIBLIOGRAFÍA

1. ISO 27001:2005 Tecnología de la Información – Técnicas de seguridad – Sistemas de seguridad de la información - Requerimientos.

2. Toro, M. 2011. Plan de seguridad de la información ISO 27002 Vs COBIT. Normas y Calidad. ICONTEC. Cuarta edición. P 26 – 28.

3. Moreno, F. 2009. La ISO/IEC 27005 en la búsqueda de información más segura. Normas y Calidad. ICONTEC. Cuarta edición. P 28 – 32.

4. ISO 27002:2005 Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

5. Orozco, E. 1995. La Inteligencia Corporativa herramienta gerencial en la lucha por la competitividad. Transferencia de Tecnología. Publicación bimensual de la Fundación Tecnológica y del Instituto Tecnológico de Costa Rica. Noviembre – Diciembre 3 (15).

6. Plantilla para aplicar el ciclo PHVA. Tomado de: http://www.negociosyemprendimiento.org/2010/08/plantilla-para-aplicar-el-ciclo-phva-de.html. [Consulta:01 Julio 2012]

7. Bestratén, M. Orriols, R. Y Mata, C. Análisis modal de fallos y efectos AMFE. Instituto Nacional de Seguridad e Higiene en el trabajo. Notas Técnicas de Prevención. 679. P 1 - 8.

8. 1 Poveda, J. Gestión y tratamiento de los riesgos, 2007. http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-9.pdf. [Consulta:01 Julio 2012]

9. Guía de seguridad de la información para pymes. Región de Murcia. 2009.

10. Carozo, E. Implantación de un sistema de gestión de seguridad de la información en una empresa compleja. Universidad de Montevideo. 2007.

11. NTC-ISO/IEC 27005, Tecnología de la información. Código de práctica para la gestión de la seguridad de la información.

12. Metodología línea base de indicadores. DANE 2009.

13. Implantación de un sistema de gestión de la seguridad de la información y certificación ISO 27001 en la Administración Pública. Tecnimap 2010.

14. NTC-ISO/IEC 17025: 2005. Requisitos generales para la competencia de laboratorios de ensayo y calibración

15. Enlaces para la familia ISO 27000 - http://www.iso27000.es/enlaces.html. [Consulta:30 Abril 2012]

16. Gerencie.com. "Auditoria de sistemas de información". Disponible: http://www.gerencie.com/auditoria-de-sistemas-de-informacion.html [citado 17 de Mayo de 2008]

17. Angelika Plate. ISO org. ISO 27001:2005. http://es.scribd.com/doc/24326153/29/ISO-IEC-27005-Anexos-Anexos [Consulta: 26 Mayo 2012]

9. ANEXOS

ANEXO 1.

DEFINICIONES

Según la ISO 27001: 2005 e ISO 27002:2005.

Activo: cualquier cosa que tenga valor para la organización.

Amenaza: una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización.

Análisis de riesgo: uso sistemático de la información para identificar las fuentes y calcular el riesgo.

Confidencialidad: La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

Control: medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. El control también se utiliza como sinónimo de salvaguarda o contramedida.

Criptografía: es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que sólo puedan ser leídos por las personas a quienes van dirigidos.

Disponibilidad: la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

Electrotecnia: es la ciencia que estudia las aplicaciones técnicas de la electricidad.

Evaluación del riesgo: proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo.

Evento de seguridad de la información: cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red, indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

Incidente de seguridad de la información: un incidente de seguridad de la información es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

Integridad: La propiedad de salvaguardar la exactitud e integridad de los activos.

Información: Es un conjunto de datos acerca de algún suceso, hecho o fenómeno, que organizados en un contexto determinado tiene su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo.

Lineamiento: descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos establecidos en las políticas.

Medios de procesamiento de la información: cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.

Métrica: es una metodología de planificación, desarrollo y mantenimiento de sistemas de información.

Política: intención y dirección general expresada formalmente por la gerencia.

Riesgo: combinación de la probabilidad de un evento y su ocurrencia.

Riesgo residual: El riesgo remanente después del tratamiento del riesgo.

Análisis de riesgo: Uso sistemático de la información para identificar fuentes y para estimar el riesgo.

Valuación del riesgo: Proceso general de análisis del riesgo y evaluación del riesgo.

Evaluación del riesgo: Proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

Tratamiento del riesgo: Proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo.

Sistema de gestión de seguridad de la información: es la parte del sistema gerencial general, basado en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Tercera persona: persona u organismo que es reconocido como independiente de las partes involucradas, con relación al ítem en cuestión.

Tratamiento del riesgo: proceso de selección e implementación de medidas para modificar el riesgo.

Vulnerabilidad: la debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

ANEXO 2.

OBJETIVOS DE CONTROL Y CONTROLES ESTABLECIDOS EN LA NORMA 17799:2005

OBJETIVOS DE CONTROL Y CONTROLES ESTABLECIDOS EN LA NORMA 17799:2005		
POLITICA DE SEGURIDAD		
Documento y revisión de la política de seguridad de la información	A.5.1, A.5.1.1 Y A5.1.2	Aprobar un documento de política de seguridad de la información, hacerlo conocer y revisar para garantizar que siga siendo adecuada, suficiente y eficaz
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
Compromiso de la dirección con la seguridad de la información	A6.1.1	La dirección debe apoyar activamente la seguridad dentro de la organización
Coordinación y asignación de responsabilidades para la seguridad de la información	A6.1.2 Y A6.1.3	Las actividades de la seguridad de la información deben ser coordinadas y definir claramente todas las responsabilidades
Procesos de autorización para los servicios de procesamiento de información	A6.1.4	Definir e implementar un proceso de autorización para nuevos servicios de procesamiento de la información
Acuerdos sobre confidencialidad	A6.1.5	Revisar los requisitos de confidencialidad
Contacto con las autoridades y con grupos de interés especiales	A6.1.6 Y A6.1.7	Mantener contactos apropiados con las autoridades pertinentes y con grupos de interés especiales
Revisión independiente de la seguridad de la información	A6.1.8	Revisar el enfoque de la organización para la gestión de la seguridad de la información
Identificación de los riesgos relacionados con las partes externas	A6.2.1	Identificar los riesgos para la información
Consideraciones de la seguridad cuando se trata con los clientes y en los acuerdos con terceras partes	A6.2.2 Y A6.2.3	Todos los requisitos de seguridad se deben considerar antes de dar acceso o hacer acuerdos
GESTIÓN DE ACTIVOS		
Inventario, propiedad y uso aceptable de los activos	A7.1.1, A7.1.2 Y A.7.1.3	Todos los activos y la información deben estar identificados y documentados
Directrices, etiquetado y manejo de la clasificación de la información	A7.2.1 Y A7.2.2	La información se debe etiquetas y clasificar teniendo en cuenta la importancia y valor

SEGURIDAD DE LOS RECURSOS HUMANOS		
Roles y responsabilidades de los empleados, selección y términos y condiciones laborales	A8.1.1, A8.1.2 Y A8.1.3	Se deben documentar los roles y responsabilidades, verificar los antecedentes de los candidatos a empleados y deben estar de acuerdo con las condiciones del contrato laboral
Responsabilidad de la dirección durante la vigencia de la contratación laboral	A8.2.1	La dirección debe exigir que se aplique la seguridad según las políticas establecidas
Educación, formación y concientización sobre la seguridad de la información	A8.2.2	Todos los empleados y terceros deben recibir formación sobre las políticas
Proceso disciplinario	A8.2.3	Debe existir un proceso disciplinario formal
Responsabilidades en la terminación del contrato laboral	A8.3.1	Asignar las responsabilidades para llevar a cabo la terminación del contrato laboral
Devolución de activos	A8.3.2	Empleados y terceros deben devolver los activos pertenecientes a la organización
Retiro de los derechos de acceso	A8.3.3	Retiro de los derechos de acceso
SEGURIDAD FISICA Y DEL ENTORNO		
Perímetro de seguridad física	A9.1.1	Se deben utilizar perímetros de seguridad, las áreas deben estar protegidas con controles de acceso, aplicar seguridad física, protecciones contra daños por desastres naturales o artificiales y aislar el acceso no autorizado
Controles de acceso físico	A9.1.2	
Seguridad de oficinas, recintos e instalaciones	A9.1.3	
Protección contra amenazas externas y ambientales	A9.1.4	
Trabajo en áreas seguras	A9.1.5	
Áreas de carga, despacho y acceso público	A9.1.6	
Ubicación y protección de los equipos	A9.2.1 Hasta A9.2.7	Los equipos deben estar protegidos y recibir mantenimiento
GESTIÓN DE COMUNICACIONES Y OPERACIONES		
Documentación de los procedimientos de operación	A10.1.1	Los procedimientos de operación se deben documentar y estar disponibles para su uso
Gestión del cambio	A10.1.2	Controlar los cambios en los servicios
Distribución de funciones	A10.1.3	Distribución de funciones
Separación de las instalaciones de desarrollo, ensayo y operación	A10.1.4	Separa las instalaciones para reducir los riesgos de cambios no autorizados
Gestión de la prestación del servicio por terceras partes	A10.2.1 Hasta A10.2.3	Garantizar que los controles, las definiciones del servicio y los niveles de prestación sean implementados, mantenidos y operados por las terceras partes.
Planificación y aceptación del sistema	A10.3.1 y A10.3.2	Hacer seguimiento y adaptación para sistemas de información nuevos
Protección contra códigos malicioso y móviles	A10.4.1 y A10.4.2	Controles de detección, prevención y recuperación.

Respaldo	A10.5	Hacer copias de respaldo
Gestión de la seguridad de las redes	A10.6.1 y A10.6.2	Mantener las redes y controlar para proteger de amenazas
Manejo de los medios	A10.7.1 Hasta A10.7.4	Establecer procedimientos para manejar los medios removibles
Intercambio de la información	A10.8.1 Hasta A10.8.5	Establecer políticas, procedimientos y controles de intercambio para proteger la información
Servicios de comercio electrónico	A10.9 y A10.10	La información involucrada en el comercio electrónico debe estar protegida contra actividades fraudulentas, disputas o modificaciones no autorizadas.
CONTROL DE ACCESO		
Requisito del negocio para el control de acceso	A.11.1	Establecer, documentar y revisar la política de control de acceso.
Gestión del acceso de usuarios	A11.2.1 Hasta A11.2.4	Asegurar el acceso a usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información
Responsabilidad de los usuarios	A11.3.1 Hasta A11.3.3	Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información
Control de acceso a las redes	A11.4.1 Hasta A11.4.7	Evitar el acceso no autorizado a los servicios de la red
Control de acceso al sistema operativo	A11.5.1 Hasta A11.5.6	Evitar el acceso al sistema operativo
Control de acceso a las aplicaciones y a la información	A11.6.1 y A11.6.2	Evitar el acceso no autorizado a la información contenida en los sistemas de información
Computación móvil y trabajo remoto	A11.7.1 y A11.7.2	Garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN		
Análisis y especificación de los requisitos de seguridad	A12.1.1	Especificar en los requisitos para los controles de seguridad las declaraciones sobre los nuevos sistemas de información o mejoras.
Procesamiento correcto en las aplicaciones	A12.2.2 Hasta A12.2.4	Evitar errores, pérdidas, modificaciones o uso inadecuado de la información en las aplicaciones.
Controles criptográficos	A12.3.3 y A12.3.2	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información

Seguridad de los archivos del sistema	A12.4.1 Hasta A12.4.3	Garantizar la seguridad de los archivos controlando la instalación de software
Seguridad en los procesos de desarrollo y soporte	A12.5.1 Hasta A12.5.5	Mantener la seguridad del software y de la información del sistema de aplicaciones
Gestión de la vulnerabilidad técnica	A12.6.1	Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas
GESTION DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN		
Reporte sobre los eventos y las debilidades de la seguridad de la información	A13.1.1 y A13.1.2	Los eventos de seguridad de la información se deben informar y todos deben reportar las debilidades observadas
Gestión de los incidentes y las mejoras en la seguridad de la información	A13.2.1 Hasta A13.2.3	Asegurar que se aplica un enfoque para la gestión de los incidentes
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
Aspectos de seguridad de la información, de la gestión de la continuidad del negocio	A14.1.1 Hasta A14.1.5	Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos
CUMPLIMIENTO		
Cumplimiento de los requisitos legales	A15.1.1 Hasta A15.1.6	Evitar el incumplimiento de cualquier ley, obligaciones y cualquier requisito de seguridad
Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico	A15.2.1 y A15.2.1	Asegurar que los sistemas cumplan las normas y políticas de seguridad
Consideraciones de la auditoría de los sistemas de información	A15.2.1 y A15.2.1	Maximizar la eficacia de los procesos de auditoría y minimizar la interferencia

ANEXO 3.

INVENTARIO DE ACTIVOS DE INFORMACIÓN

ANEXO 3

LOGO DE LA ORGANIZACIÓN	INVENTARIO DE ACTIVOS DE INFORMACIÓN	CÓDIGO:
		FECHA DE EMISIÓN
		PAGINA

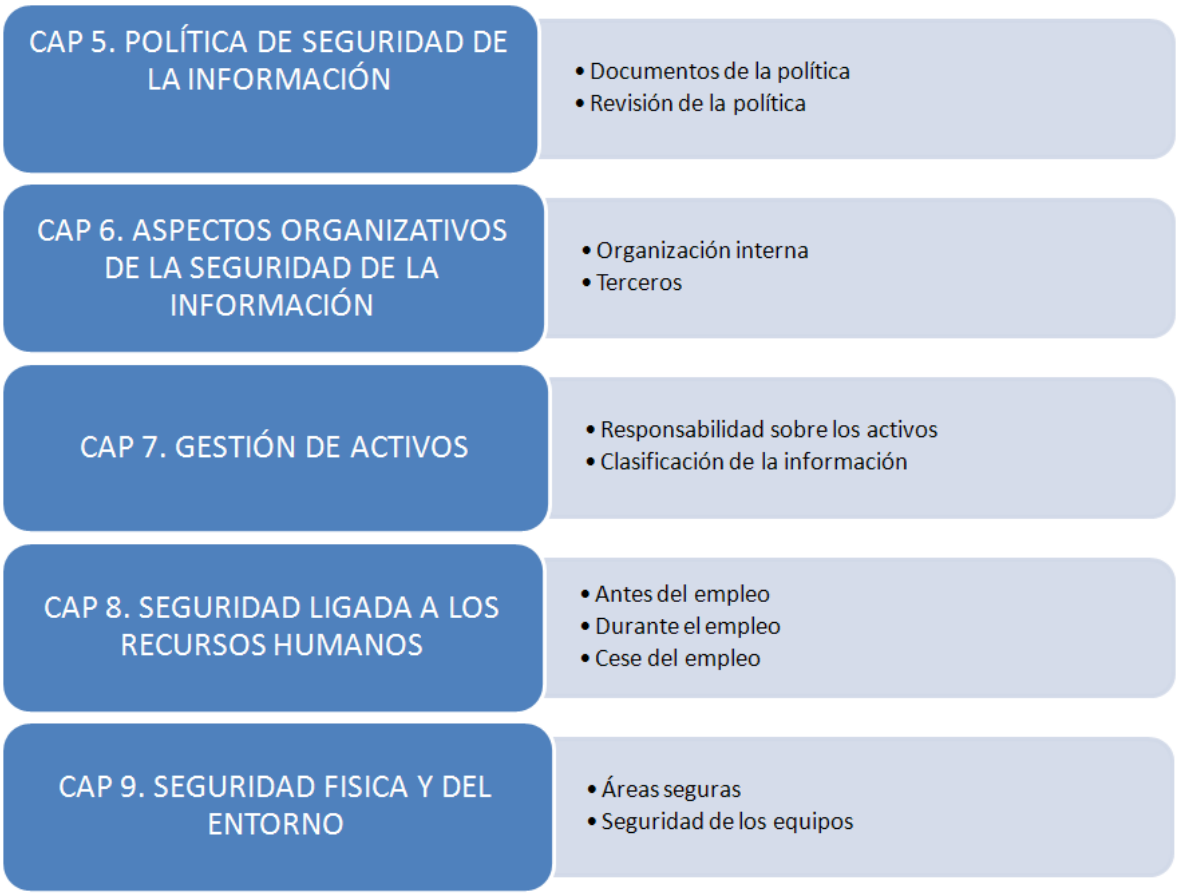
PROCESO	IDENTIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	PROPIETARIO/ RESPONSABLE	UBICACIÓN	C	I	A

C: Confiabilidad I: Integridad A: Disponibilidad

ELABORADO POR:_____ APROBADO POR: _____

ANEXO 4.

CONTROLES DE SEGURIDAD ISO/IEC 2002: 2008



Fuente: Los autores.

ANEXO 5.

HERRAMIENTAS PROPUESTAS PARA LA ETAPA DE VERIFICAR. CONTROL EN EL SGSI.

1. GRÁFICOS DE CONTROL

Esta herramienta es de gran utilidad en el momento del análisis de tendencias de los indicadores trazados. Consiste en determinar gráficamente los límites bajo los cuales se considera que determinado indicador está bajo control o dentro de las especificaciones aceptadas tal como se muestra a continuación.

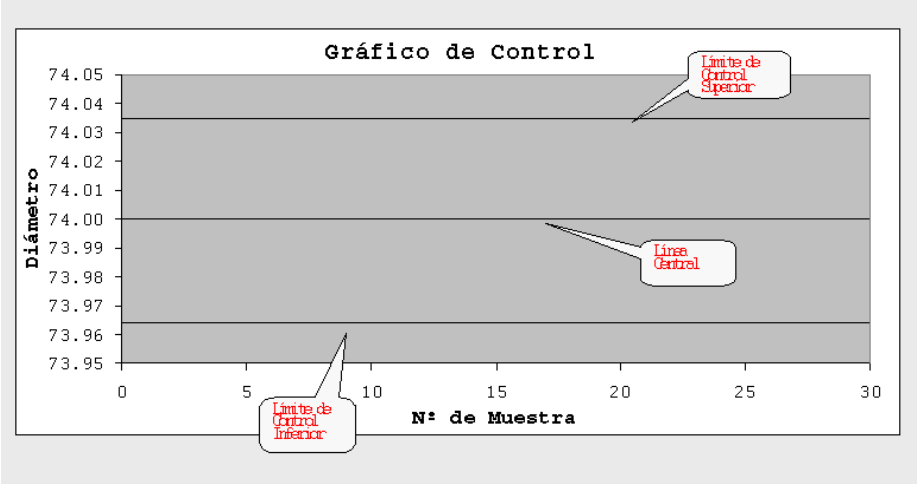


Ilustración 9 Grafico de control. Limites.

Fuente: Escuela Colombiana de Ingeniería,/Diplomado Six Sigma 2009

Una vez construida la plantilla se grafica los valores de la medición realizada,

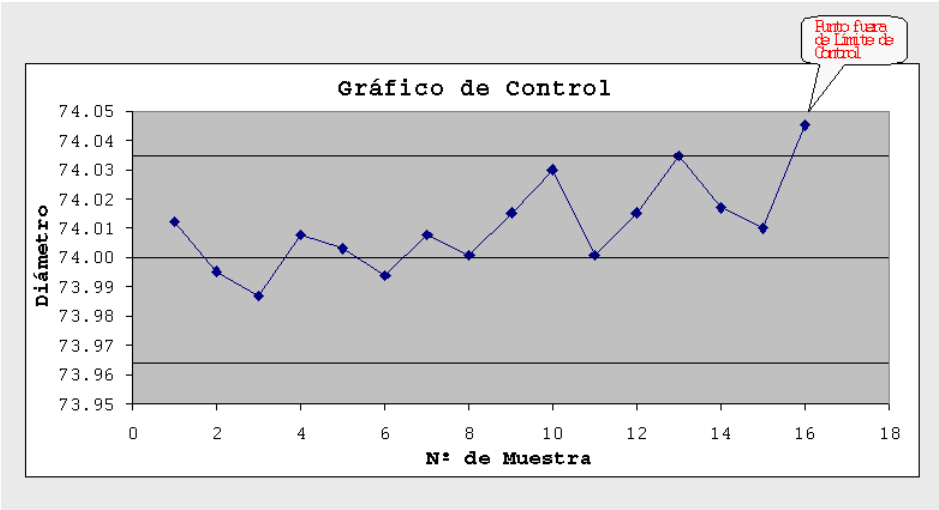


Ilustración 10 Grafico de Control. Punto fuera de especificación

Fuente: Escuela Colombiana de Ingeniería,/Diplomado Six Sigma 2009

después del séptimo dato se puede empezar a analizar las tendencias del indicador con el fin de tomar decisiones, a continuación se enuncia comportamientos típicos y como analizarlos.

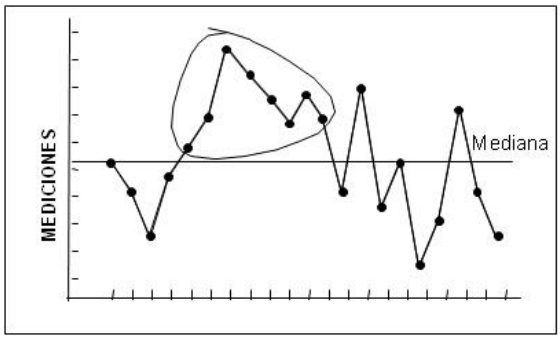


Ilustración 11 Grafico de Control. Analisis respecto a la Mediana.

Fuente: Escuela Colombiana de Ingeniería,/Diplomado Six Sigma 2009

Siete o más puntos seguidos en el mismo lado de la mediana indican una variación en el proceso. (Si los datos son simétricos se puede usar la media como promedio en lugar de la mediana).

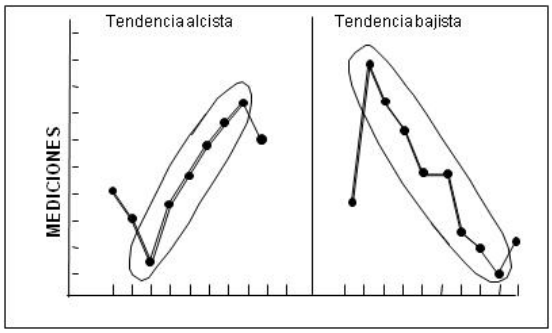


Ilustración 12 Gráfica de Control. Tendencias.

Fuente: Escuela Colombiana de Ingeniería,/Diplomado Six Sigma 2009

- Seis o más puntos seguidos con incremento o decremento continuo indican una tendencia. (Se debe empezar a contar en el punto en el que cambia la dirección).

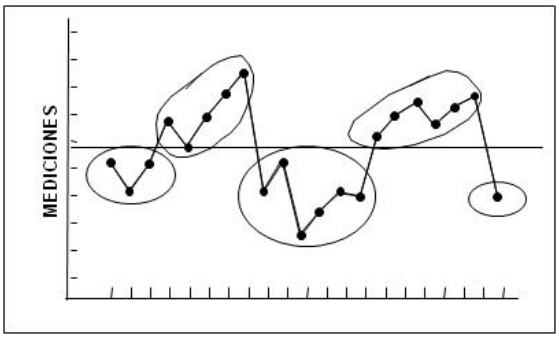


Ilustración 13 Gráfica de Control. Tendencias.

Fuente: Escuela Colombiana de Ingeniería,/Diplomado Six Sigma 2009

- Muy pocos datos agrupados indican una desviación en la media del proceso, un ciclo o una tendencia.
- Demasiados datos agrupados indican muestreo desde dos fuentes, sobrecompensación o un sesgo.

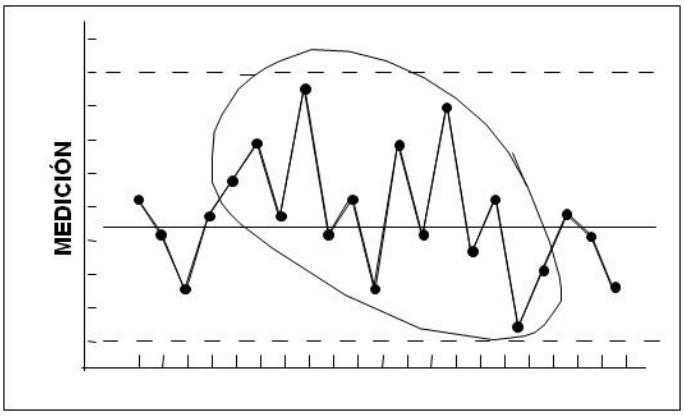


Ilustración 14 Gráfica de Control. Dispersión.

Fuente: Escuela Colombiana de Ingeniería,/Diplomado Six Sigma 2009

- 14 o más puntos seguidos alternando arriba y abajo indican problemas de sesgo o de muestreo.

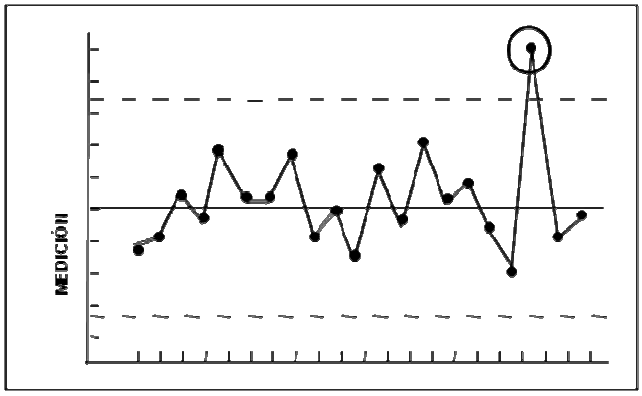


Ilustración 15 Gráfica de Control. Dispersión.

Fuente: Escuela Colombiana de Ingeniería,/Diplomado Six Sigma 2009

- Uno o más puntos fuera de los límites de control indican una diferencia en estos puntos.

El análisis de los datos y tendencias permiten anticiparse con acciones preventivas a hechos que más adelante pueden causar problemas el interior de SGSI. Un adecuado seguimiento garantiza acciones oportunas.

2. PLAN DE VERIFICACIÓN DEL SGSI

Este documento especifica los procesos, procedimientos, riesgos, controles, responsables, objetivos de control y los indicadores como herramienta para evaluar la eficiencia y establecer el cumplimiento de los requisitos del SGSI. El plan propuesto en la tabla 9, establece el resultado de la planificación del SGSI, con base en el alcance y los objetivos del sistema.

Tabla 10 Plan de verificación del SGSI Fuente: Los autores

LOGO DE LA ORGANIZACIÓN		PLAN DE VERIFICACIÓN DEL SGSI						
		ALCANCE:						
		OBJETIVOS DEL SGSI:						
Nombre del proceso	Diagrama de flujo del proceso	Procedimiento	Riesgo a controlar	Metodo de control de proceso			Objetivo de control	Indicador
				Control implementado	Registro	Responsable		

3. BALANCED SCORECARD O CUADRO DE MANDO INTEGRAL

El BSC es una herramienta analítica que permite monitorear los indicadores financieros, la perspectiva de los clientes, los procesos internos y determinar los temas de capacitación y formación necesarios para llevar a cabo las estrategias de la organización, en este caso en términos del sistema de gestión de seguridad de la información.

El Balanced Scorecard permite alinear los objetivos, indicadores, metas y planes de acción, además promueve que todos los miembros de la organización entiendan y estén alineados a la estrategia.

Cuando la organización adquiere cierta experiencia en el manejo de métricas, puede encontrar útil desarrollar un cuadro de mando (Tabla 10). Un cuadro de mando consiste en la gestión del conjunto de indicadores que son establecidos en la etapa del “hacer” y que sirven para tomar

decisiones al respecto, teniendo en cuenta no solo los procesos internos del laboratorio sino el ámbito financiero, el cliente y el aprendizaje (Dane, 2009).

Tabla 11 Cuadro de Mando Integral aplicado al SGSI Fuente: Los autores

CUADRO DE MANDO INTEGRAL APLICADO AL SGSI								
	OBJETIVOS	INDICADOR DE RESULTADOS	UNIDAD	META	PLAZO	INDICADORES DE ACTUACIÓN	INICIATIVA ESTRATEGICA (acciones)	INICIATIVA ESTRATEGICA (responsables)
PERSPECTIVA								
Financiera								
Clientes								
Procesos internos								
Aprendizaje Organizacional								

ANEXO 6.

HERRAMIENTAS PROPUESTAS PARA LA ETAPA DEL ACTUAR. ANÁLISIS Y GENERACION DE ACCIONES EN EL SGSI.

1. DIAGRAMA CAUSA-EFECTO

Muy útil para causas de un problema determinado, la metodología consiste en reunir un grupo interdisciplinar que esté involucrado en el proceso, evaluar cada una de las variables que pueden llegar a afectar el resultado de la operación en que se detecto el problema (Mano de obre, Maquina, Material, Métodos, etc) cualquier variable puede incluirse dentro del diagrama, las anteriores son las más comunes pero el grupo está en la facultad de manejar las variables a analizar según considere conveniente.

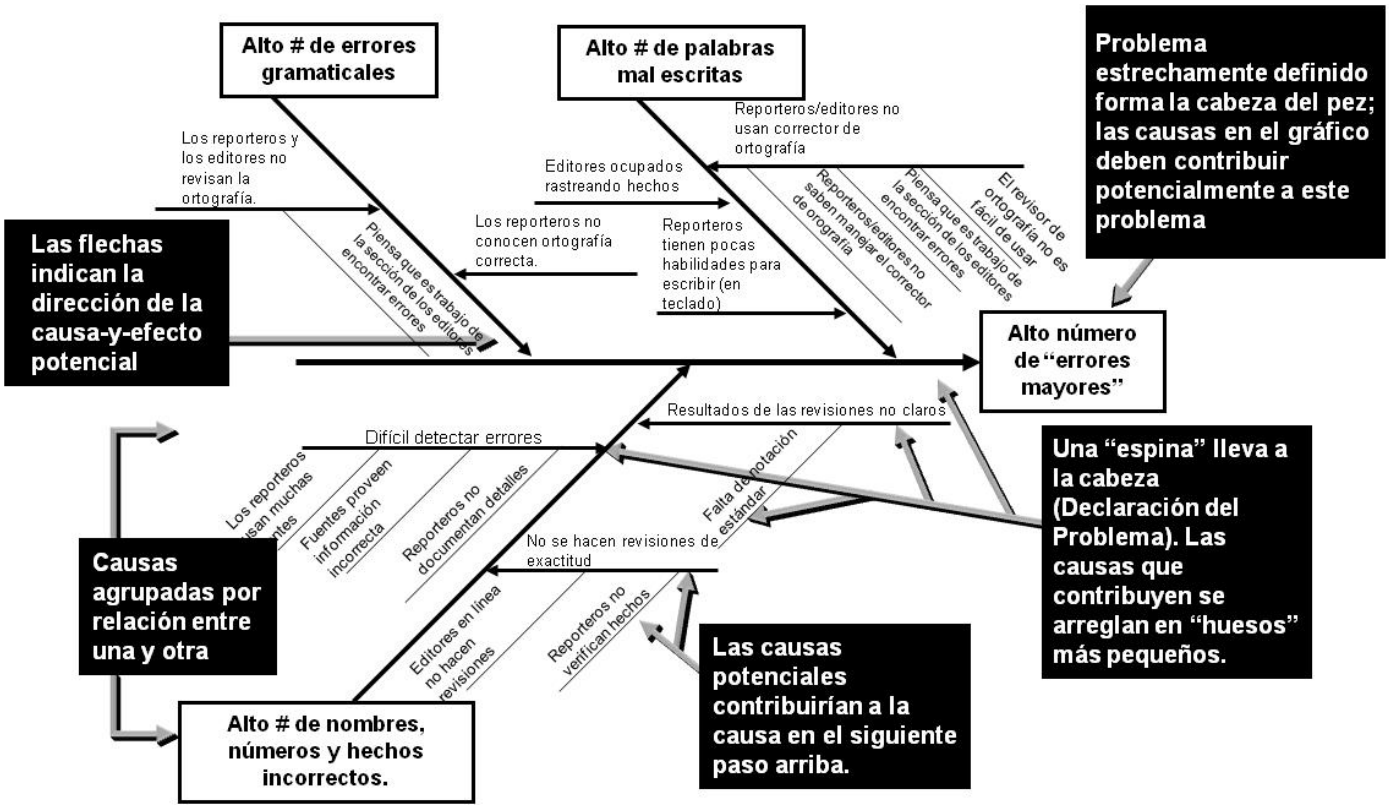


Ilustración 16 Diagrama Causa-Efecto

Fuente: Escuela Colombiana de Ingeniería,/Diplomado Six Sigma 2009

La grafía anterior muestra la construcción del diagrama, el problema es la cabeza del mismo de la cual salen las variables a analizar, una en cada espina principal.

Se realiza entonces una lluvia de ideas para asignar una posible causa del problema principal en cada una de las variables analizadas, en adelante se debe repetir el proceso para identificar 2 o 3 sub causas de la causa principal determinada para cada variable. De esta forma van surgiendo diferentes posibles causas del problema a solucionar, una vez se lleve el cuadro con 3 niveles de profundidad, se deben priorizar cuales de las causas encontradas atacar teniendo en cuenta la complejidad y el impacto de atacar una o la otra.

2. LOS 5 ¿Por qué?

Esta metodología complementa al diagrama causa efecto, trabajándolas unidas hacen una herramienta muy efectiva en la detección de causa raíz de un problema.

El diagrama de causa efecto se determinan diferentes posibles causas de un determinado problema, los 5 porque consiste en preguntar como mínimo 5 veces ¿Por qué sucede determinada causa?, dando respuesta a 5 porque's se llega a un nivel de profundidad que permite determinar la causa raíz del problema. Una acción para mitigar una causa raíz asegura que el problema desaparezca y no se vuelva a repetir.

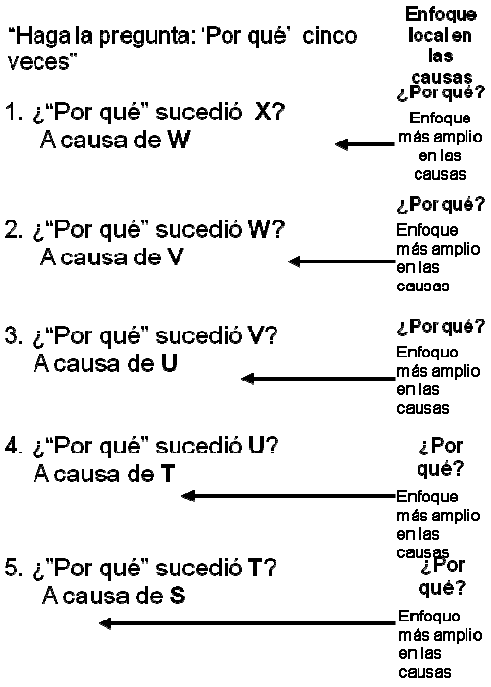


Ilustración 17 Los 5 ¿Por qué?

Fuente: Escuela Colombiana de Ingeniería,/Diplomado Six Sigma 2009

Las anteriores dos herramientas se proponen para determinar de manera efectiva en que gastar esfuerzos en el momento de lanzar acciones correctivas y preventivas, las acciones como tal dependen del tipo de problema, no existe una metodología para determinar la forma de proceder para resolver determinado problema, esto depende de la creatividad y conocimiento del grupo dispuesto para buscar la solución.

LICENCIA DE USO – AUTORIZACIÓN DE LOS AUTORES

Actuando en nombre propio identificado (s) de la siguiente forma:

Nombre Completo Carol Estefanie Murillo Varon

Tipo de documento de identidad: C.C. ☒ T.I. ☐ C.E. ☐ Número: 1110445863

Nombre Completo Diego Hernando Bonilla Pineda

Tipo de documento de identidad: C.C. ☒ T.I. ☐ C.E. ☐ Número: 80820265

Nombre Completo Johanna Cardina Buitrago Estrada.

Tipo de documento de identidad: C.C. ☒ T.I. ☐ C.E. ☐ Número: 52965338

Nombre Completo

Tipo de documento de identidad: C.C. ☐ T.I. ☐ C.E. ☐ Número:

El (Los) suscrito(s) en calidad de autor (es) del trabajo de tesis, monografía o trabajo de grado, documento de investigación, denominado:

Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información - 5651:, en el sector de laboratorios de análisis microbiológicos, basado en ISO 27001

Dejo (dejamos) constancia que la obra contiene información confidencial, secreta o similar: SI ☐ NO ☒
(Si marqué (marcamos) SI, en un documento adjunto explicaremos tal condición, para que la Universidad EAN mantenga restricción de acceso sobre la obra).

Por medio del presente escrito autorizo (autorizamos) a la Universidad EAN, a los usuarios de la Biblioteca de la Universidad EAN y a los usuarios de bases de datos y sitios webs con los cuales la Institución tenga convenio, a ejercer las siguientes atribuciones sobre la obra anteriormente mencionada:

A. Conservación de los ejemplares en la Biblioteca de la Universidad EAN.
B. Comunicación pública de la obra por cualquier medio, incluyendo Internet
C. Reproducción bajo cualquier formato que se conozca actualmente o que se conozca en el futuro
D. Que los ejemplares sean consultados en medio electrónico
E. Inclusión en bases de datos o redes o sitios web con los cuales la Universidad EAN tenga convenio con las mismas facultades y limitaciones que se expresan en este documento
F. Distribución y consulta de la obra a las entidades con las cuales la Universidad EAN tenga convenio

Con el debido respeto de los derechos patrimoniales y morales de la obra, la presente licencia se otorga a título gratuito, de conformidad con la normatividad vigente en la materia y teniendo en cuenta que la Universidad EAN busca difundir y promover la formación académica, la enseñanza y el espíritu investigativo y emprendedor.

Manifiesto (manifestamos) que la obra objeto de la presente autorización es original, el (los) suscritos es (son) el (los) autor (es) exclusivo (s), fue producto de mi (nuestro) ingenio y esfuerzo personal y la realizó (zamos) sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de exclusiva autoría y tengo (tenemos) la titularidad sobre la misma. En vista de lo expuesto, asumo (asumimos) la total responsabilidad sobre la elaboración, presentación y contenidos de la obra, eximiendo de cualquier responsabilidad a la Universidad EAN por estos aspectos.

En constancia suscribimos el presente documento en la ciudad de Bogotá D.C.,

NOMBRE COMPLETO: Carol Estefanie Murillo V.
FIRMA: _____
DOCUMENTO DE IDENTIDAD: 1110445863
FACULTAD: Postgrado
PROGRAMA ACADÉMICO: Esp. Procesos y Calidad

NOMBRE COMPLETO: Diego Hernando Bonilla. P.
FIRMA: _____
DOCUMENTO DE IDENTIDAD: 80820265
FACULTAD: Postgrado
PROGRAMA ACADÉMICO: Esp. Procesos y Calidad.

NOMBRE COMPLETO: Johanna Cardina. Buitrago. E
FIRMA: _____
DOCUMENTO DE IDENTIDAD: 52.965.338
FACULTAD: Postgrado
PROGRAMA ACADÉMICO: Esp. Procesos y Calidad

NOMBRE COMPLETO: _____
FIRMA: _____
DOCUMENTO DE IDENTIDAD: _____
FACULTAD: _____
PROGRAMA ACADÉMICO: _____

Fecha de firma: 23 de julio de 2012