ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL

TESIS DE GRADO

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

Analista en Sistemas

TEMA:

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL AREA DE RECURSOS HUMANOS

AUTOR(ES):

BETTY LUNA MATAMOROS
RONALD ORTÍZ RODRÍGUEZ
JAIME PAREDES ARTEAGA

DIRECTOR:

ING. VICTOR MUÑOZ

Año

2011

AGRADECIMIENTO

Agradecemos a nuestro Dios, por cada día de vida y por las oportunidades puestas en nuestro camino y haber llegado a nuestra meta.

Agradecemos a nuestras madres, por la paciencia y ternura de nuestros primeros pasos, por su guía y apoyo incansable durante estos años; por su amor incomparable.

Agradecemos a nuestros padres, por el apoyo brindado y por ese aliento de fuerza cuando nos veían flaquear en el camino; por su orgullo mal disimulado en cada obstáculo que dejábamos atrás.

Agradecemos a nuestros hermanos, por su compañía en esta vida, por ser amigos y confidentes, por simplemente estar allí.

DEDICATORIA

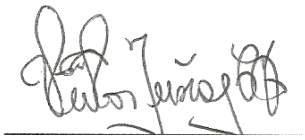
Nos llena de alegría el poder dedicarle esta tesis a nuestro Dios que nos ha dado las fuerzas necesarias para poder llegar al final.

A nuestras familias, a cada uno de sus miembros, ya que de una u otra manera han colaborado durante estos años a que no nos rindamos en el intento de superación al que nos comprometimos al inicio de nuestras carreras.

DECLARACIÓN EXPRESA

La responsabilidad del contenido de este Trabajo Final de Graduación, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral.

Firma del Director del Proyecto
y Miembros del Tribunal

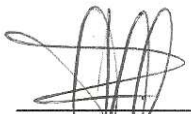


Ing. Víctor Muñoz

Director del Proyecto

Delegado

Firma de los Autores del Proyecto de Graduación



Betty Luna Matamoros

Ronald Ortiz Rodríguez

Jaime Paredes Arteaga

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

INTRODUCCIÓN

1 INTRODUCCIÓN

1.1 ¿QUÉ ES SEGURIDAD DE LA INFORMACIÓN?

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistema tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad y Integridad de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial.

Esta ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, Planificación de la continuidad del negocio, Ciencia Forense Digital y Administración de Sistemas de Gestión de Seguridad por nombrar algunos.

La necesidad de proteger los datos personales excede el mero interés del Hospital del Niño Francisco Icaza Bustamante, (en adelante El Organismo).

Desde hace más de una década la legislación protege el honor y la intimidad de los datos personales y familiares. Primero mediante la derogada Ley Orgánica 5/1992 conocida como LORTAD, y más recientemente con la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, conocida como LOPD. La LOPD otorga una serie de derechos a las personas cuyos datos sean objeto de tratamiento, y establece las obligaciones de quienes efectúen dichos tratamientos.

Información como el sueldo de los empleados, desempeño profesional o bajas laborales, pertenece al departamento de Recursos Humanos y es considerada confidencial en cualquier sector.

Por la naturaleza intrínseca de los datos de Recursos Humanos las obligaciones establecidas en la LOPD deben ser consideradas con sumo rigor.

1.2 MARCO DE REFERENCIA

1.2.1 ¿Qué es un SGSI?

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

El propósito de un sistema de gestión de la seguridad de la información no es garantizar la seguridad (que nunca podrá ser absoluta) sino garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías.

La seguridad de la información, según ISO 27001, consiste en la preservación de su ***confidencialidad, integridad, disponibilidad y legalidad***, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos cuatro términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- ***Integridad***: Mantener la exactitud y completitud de la información y sus métodos de proceso.

- ***Privacidad***: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- ***Legalidad***: La información debe de cumplir con las leyes vigentes dependiendo del lugar donde se encuentran y son manejadas.

- ***Disponibilidad***: El acceso y la utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Fig. F1 SGSI Principios básicos.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

1.2.2 ISO (International Organization for Standardization)

La ISO es una federación internacional con sede en Ginebra (Suiza) de los institutos de normalización de 157 países (uno por cada país). Es una organización no gubernamental (sus miembros no son delegados de gobiernos nacionales), puesto que el origen de los institutos de normalización nacionales es diferente en cada país (entidad pública, privada).

La ISO desarrolla estándares requeridos por el mercado que representan un consenso de sus miembros (previo consenso nacional entre industrias, expertos, gobierno, usuarios, consumidores) acerca de productos, tecnologías, sistemas y métodos de gestión, entre otros.

Estos estándares, por naturaleza, son de aplicación voluntaria, ya que el carácter no gubernamental de ISO no le da autoridad legal para forzar su implantación. Sólo en aquellos casos en los que un país ha decidido adoptar un determinado estándar como parte de su legislación, puede convertirse en obligatorio.

La ISO garantiza un marco de amplia aceptación mundial a través de sus 3.000 grupos técnicos y más de 50.000 expertos que colaboran en el desarrollo de estándares.

1.2.2.1 ISO 27000

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001.

Su origen lo explicaremos más adelante dentro de los anexos del documento.

1.2.3Metodología ISO27001

Es un estándar ISO que proporciona un modelo para establecer, implementar, utilizar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en el ciclo de vida PDCA (Planear-Hacer-Verificar-Actuar; o ciclo de Deming) de mejora continua, al igual que otras normas de sistemas de gestión (ISO 9001 para calidad, ISO 14001 para medio ambiente, etc.).

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

- ***Alcance del SGSI:*** ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGS considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

- ***Política y objetivos de seguridad***: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

- ***Procedimientos y mecanismos de control que soportan al SGSI:*** aquellos procedimientos que regulan el propio funcionamiento del SGSI. Documentación necesaria para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados -Métricas.

- ***Enfoque de evaluación de riesgos:*** descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro

del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables .

- ***Informe de evaluación de riesgos:*** estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

- ***Plan de tratamiento de riesgos:*** documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

- ***Procedimientos documentados:*** todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

- ***Registros:*** documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

- ***Declaración de aplicabilidad:*** (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

1.2.3.1¿Cómo se implementa un SGSI?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

• ***Plan (planificar):*** establecer el SGSI.

• ***Do (hacer):*** implementar y utilizar el SGSI.

• ***Check (verificar):*** monitorizar y revisar el SGSI.

• ***Act (actuar):*** mantener y mejorar el SGSI.

.

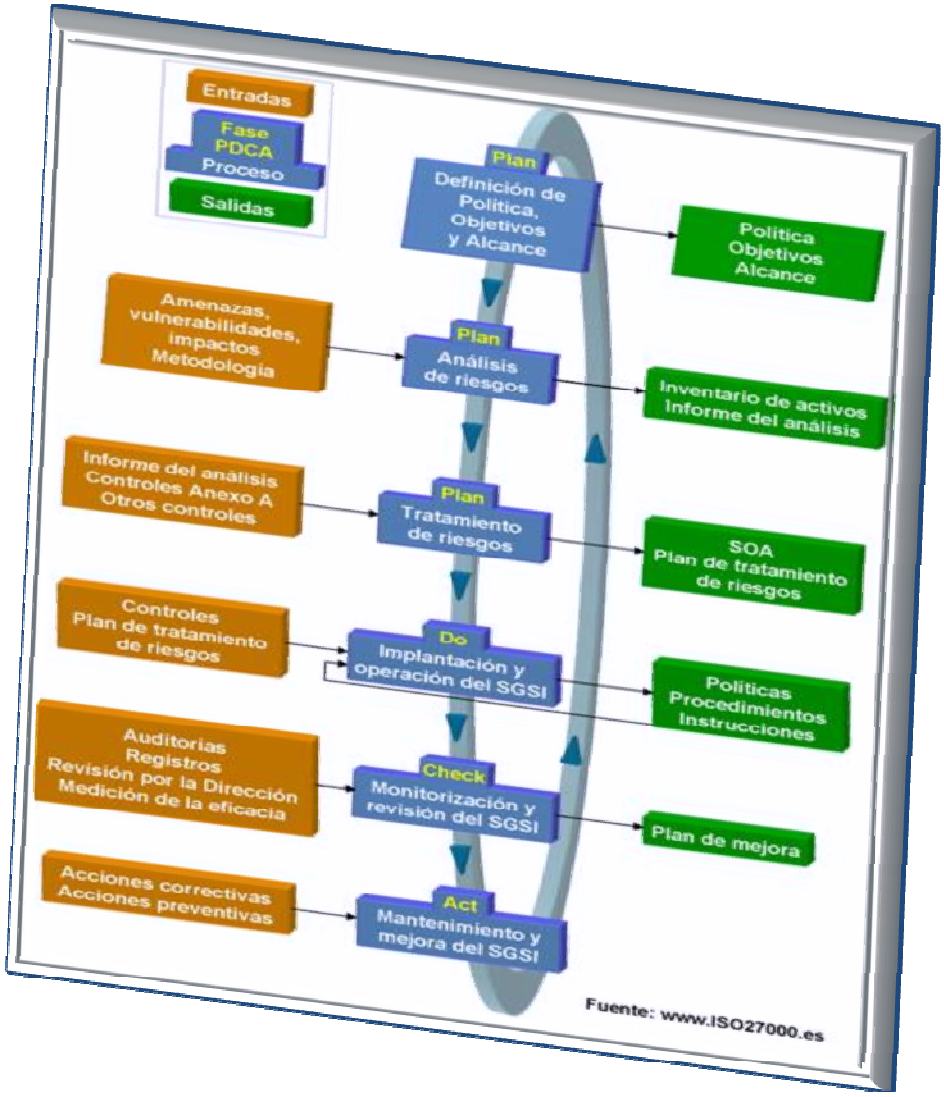


Fig. F.2 Plan-Do-Check-Act – Fuente: www.ISO27000.es

1.2.3.2La seguridad en los Recursos Humanos

La gestión de la seguridad de la información, al igual que la mayoría de los ámbitos de la gestión empresarial, depende principalmente de las personas que componen la Organización. La información sólo tiene sentido cuando es utilizada por las personas y son estas, quienes en último término, deben gestionar adecuadamente este importante recurso de la empresa. Por tanto, no se puede proteger adecuadamente la información sin una correcta gestión de los Recursos Humanos.

Pero sin duda, una de las áreas que más importancia tiene en la seguridad de la información es el departamento encargado de gestionar los Recursos Humanos.
Aspectos como la formación de los empleados, la captación y selección de nuevos miembros de la plantilla, la gestión de empleados que abandonan la Organización o la implementación de la normativa interna, son fundamentales en el tema que nos ocupa.

Todas las claves que se van a desarrollar en el presente artículo, se podrían resumir en una sola frase: conseguir que los criterios de seguridad estén presentes en la gestión de los Recursos Humanos. Un magnífico punto de partida podría ser que los responsables de Seguridad y Recursos Humanos se sienten juntos y compartan impresiones.

Entre tanto, podemos anticipar algunos aspectos fundamentales a tener en cuenta. Reclutamiento y salida de empleados.

Existen dos puntos fundamentales en el ciclo de vida de todo empleado en una Organización: El inicio de su actividad profesional y la finalización de la misma.

1.2.3.2.1 *Reclutamiento*

Cada nuevo empleado de la Organización es una apuesta de futuro. La empresa asigna una serie de tareas y responsabilidades al nuevo empleado, y proporciona los medios materiales y la información necesaria para que pueda llevarlas a cabo. Debe existir un procedimiento de reclutamiento que tenga en cuenta los siguientes aspectos relativos a la seguridad:

Definición del puesto: Para cada nueva vacante se debe definir la criticidad del puesto a cubrir según su responsabilidad y la información que maneja. Cada empresa debe definir su criterio propio. Algunos puestos críticos pueden ser directivos, personal de seguridad, personal de contabilidad, etc.

Selección: En la selección de candidatos a puestos críticos se deben comprobar los antecedentes penales y las referencias profesionales.

Contrato: El contrato laboral debe incluir los correspondientes acuerdos de confidencialidad, propiedad intelectual y protección de datos.

Comienzo: Durante los primeros días de trabajo, es recomendable que el empleado:

- Asista a unas sesiones de formación donde se le introduzca en la normativa interna y de seguridad de la empresa. De este modo todo empleado conoce sus obligaciones de seguridad tales como la protección de sus claves de acceso, uso adecuado del email e internet, clasificación de la información, etc.
- Reciba el manual de normativa interna y firme el compromiso de cumplimiento del mismo. Este trámite establece formalmente las normas internas y garantiza que el empleado conoce la normativa existente.

Accesos: Los accesos a la información y sistemas informáticos deben ser solicitados siempre por el responsable directo del empleado al departamento Centro de Cómputo. Dichos accesos deben ser siempre justificables por la labor que se va a realizar, y en caso de ser privilegiados, el Departamento de Seguridad debe aprobar su concesión.

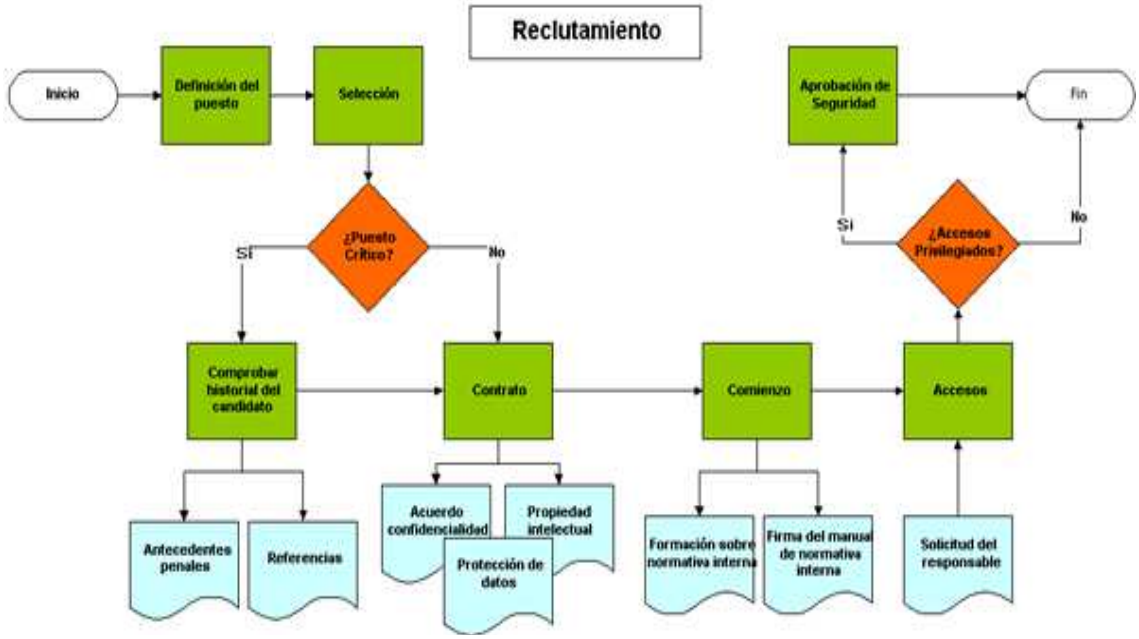


Fig. F.3 Reclutamiento de personal

1.2.3.2.2 *Salida de empleados*

La salida de un empleado es un punto crítico de riesgo para la Organización. En casos de problemas laborales y despidos, un empleado modelo hasta la fecha, puede convertirse en una seria amenaza. La historia reciente está plagada de casos de sabotaje o substracción de información por parte de empleados disgustados".

Lamentablemente, es bastante común que no se gestionen coordinadamente las bajas de los empleados. En muchas ocasiones, Recursos Humanos se encarga de realizar los trámites legales de la baja, mientras que el responsable del empleado es quien trata directamente con él y planifica el traspaso de su trabajo. Por otro lado, IT se ocupa de dar de baja sus accesos (en el momento en que perciben su ausencia). Este escenario acaba degenerando en problemas tales como que los accesos de los ex empleados siguen vigentes durante meses, o que tras la marcha del empleado no es posible recuperar cierta información vital que poseía. Para evitar todo esto, debe existir un procedimiento de bajas que tenga en cuenta los siguientes aspectos de seguridad:

Clasificación de las bajas: El responsable del empleado junto con Recursos Humanos debe clasificar la baja según las circunstancias que la rodean. Un ejemplo de posibles categorías sería:

- Renuncia
- Muerte
- Jubilación obligatoria
- Jubilación anticipada
- Destitución
  - Sumario administrativo
  - Sanción
- Supresión de puestos

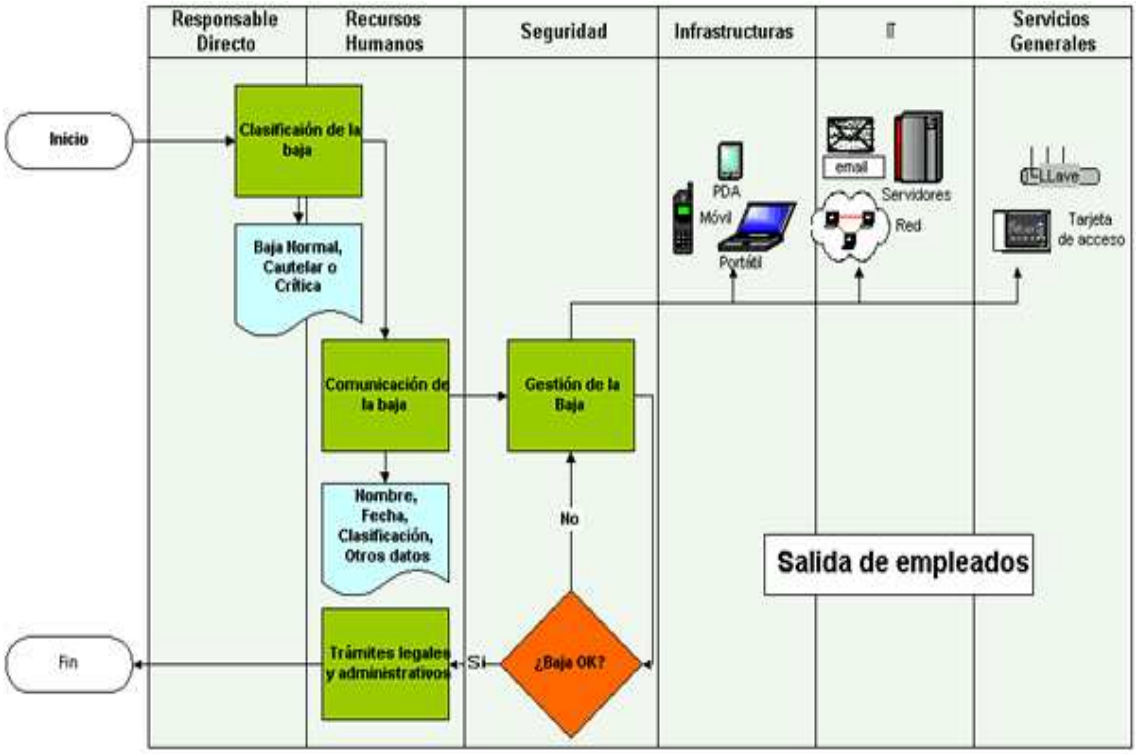


Fig. F.4 Cese de funciones

CAPÍTULO 2

BREVE HISTORIA DE LA EMPRESA

2 BREVE HISTORIA DE LA EMPRESA

2.1 HOSPITAL DEL NIÑO FRANCISCO ICAZA BUSTAMANTE

2.1.1Reseña histórica

La fecha de fundación e historia. El Hospital del Niño Dr. Francisco de Icaza Bustamante inauguró la consulta externa el 11 de enero de 1982, y hospitalización el 7 de octubre de 1985.

La comunidad guayaquileña caracterizada por enfrentar grandes desafíos, reunida el mes de diciembre de 1951, en el club de leones analizando los múltiples problemas de la ciudad encontró eco en la voz del Dr. Rosendo Arosemena Elizalde, quien plantea la necesidad de construir un nuevo hospital pediátrico para atender a los niños pobres de Guayaquil.

La idea fue descartada inicialmente por la magnitud que la obra significaba.

Fue el Sr. Alberto Enríquez navarro, quien con profunda fe convence a la directiva para encargar este gran problema, y recogiendo el reto como propio propuso asumir la empresa mediante la creación de un comité especial, nace entonces en el mes de febrero de 1952, el comité pre-construcción del moderno Hospital del Niño del Club de Leones de Guayaquil, teniendo como Director Ejecutivo al mencionado señor Alberto Enríquez Navarro; acompañado en otras dignidades por los señores: Dr. Francisco de Icaza Bustamante, Presidente de honor, Sr. Julio C. Moreno: presidente del Club de Leones, Sr. Jorge Chiriboga Founes: Subdirector, Dr. Rosendo Arosemena Elizalde: Coordinador, Dr. Alfredo Valenzuela Barriga: Asesor médico, Dr. Wenceslao Nowak Ycaza Cornejo, Tesorero Dr. Rigoberto Ortiz Bermeo: Sindico, Dr. Raúl Clemente Huerta: Comisionado de Finanzas, Sr. Francisco Illingworth Icaza: Comisionado técnico y otros distinguidos caballeros representantes de las sociedades médicas de la ciudad y de la prensa escrita.

2.1.2Justificación

La grave crisis de salud en el país demanda la necesidad de intensificar la modernización del sector y el fortalecimiento institucional del Ministerio de Salud Pública, que auné esfuerzo y recursos entre sí y con otros sectores en procura de contribuir al óptimo aprovechamiento de los escasos recursos para el mejoramiento de las condiciones de salud y de vida de toda la población.

2.1.3Visión

Ser líderes en el país en atención pediátrica y juvenil con recursos humanos altamente calificado, motivado, humanizado con educación continua gestionando recursos financieros que nos permiten contar tecnología de punta con un sistema de referencia y contra referencia implementando, coordinando acciones interinstitucionales y de participación comunitaria.

2.1.4Misión

Brindar servicios de atención pediatría y de subespecialidades, clínica, Quirúrgica: Ambulatoria, hospitalización y emergencia. Las 24 horas al día en salud integral con calidad, calidez, eficiencia y efectividad a la población menor de 15 años del país.

2.1.5Ubicación

Las instalaciones del Hospital Francisco Icaza Bustamante están ubicadas en las calles Avda. Quito y Gómez Rendón

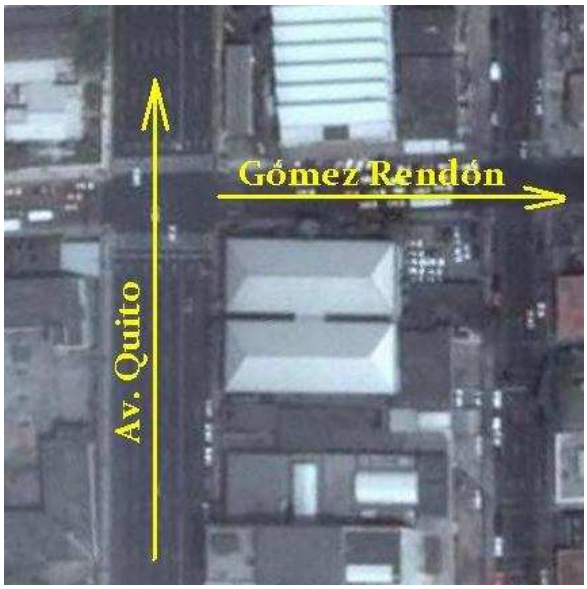


Fig. F.5 Mapa de ubicación

2.2 ORGANIZACIÓN

El Hospital Francisco Icaza Bustamante es uno de los más grandes a nivel nacional, atendiendo no solo a pacientes de la región, sino que también existen pequeños de otras provincias que necesitan ser atendidos en sus instalaciones, para ello, existen actualmente 1.300 trabajadores que desempeñan sus funciones en el Hospital del Niño Francisco Icaza Bustamante; incluyendo:

-Médicos generales

-Médicos especialista

-Trabajadores de mantenimiento

-Trabajadores de servicios generales

-Administrativo

La máxima autoridad dentro de la Organización es el Director general, teniendo a su vez la Subdirección Médica y la Subdirección Administrativa dirigiendo cada una de las subdivisiones establecidas. Los empleados están divididos dependiendo su desempeño bajo una de las subdirecciones respectivamente.

Existen actualmente 17 áreas establecidas dentro del funcionamiento del Organismos, de las cuales 5 están bajo las normas del Código de Trabajo ya que sus funciones no son del ámbito profesional sino más bien dirigido hacia los Servicios Varios que se desempeñan en el mismo, por lo que no son incluidos en los de carácter profesional.

Todas las decisiones que se toman con respecto al personal se rigen bajo la Ley Orgánica de Servicio Público (LOSEP); y cada proceso que se inicia esta supervisado por la Subsecretaría de Desarrollo Civil de RRHH y por el Ministerio de Recursos Humanos, quienes conjuntamente con la dirección del Hospital elaboran instructivos para el Sistema de Integración de RRHH, basados en los siguientes Items:

- Reclutamiento y Selección
  - -Norma técnica de selección y concurso
  - -Instructivo para llenar vacante
- Clasificación de puestos
  - -Una vez al año, Analistas del ministerio actualizan la tabla de clasificación de puestos bajos una norma técnica para evaluar cada uno de los puestos establecidos y su óptimo funcionamiento.
- Sistema de evaluación de desempeño
  - -Existen grados de evaluación de cada uno de los trabajadores, tabla que va desde (excelente… deficiente) la misma que es usada para examinar las funciones de los empleados, en la que se podrá otorgar un ascenso o en una baja laboral dependiendo de cada caso en particular.

- Capacitación
  - -Una vez al año el jefe de cada área propone un cuadro de capacitación para los elementos de su área y asi mantener la eficiencia de su alternos, capacitación que es de carácter obligatoria para el continuo funcionamiento de sus funciones.
- Planificación de RRHH
  - -Anualmente se realiza un estudio en la que se evalúa la necesidad de la creación de puestos o la de suprimir puestos o la de fusión de los mismos.

2.2.1Clasificación de contratos

Actualmente los contratos laborales son determinados dependiendo de las funciones a ejercer y las necesidades que existen para cubrir las vacantes. El jefe de área es quien comunica la necesidad de cubrir un puesto específico, el Director General es quien otorga el consentimiento y es el responsable directo de la convocatoria a concurso para cubrir la plaza disponible.

Todas las plazas son cubiertas mediante el sistema de merecimiento y oposición en el cuál los aspirantes se someten a evaluaciones específicas, quedando seleccionado el más idóneo dependiendo de las calificaciones obtenidas.

- Nombramiento ganador de concurso indefinido
- Nombramiento ganador de concurso a plazo fijo
- Nombramiento provisional
- Contratos ocasionales

2.2.2Clasificación de bajas

La tabla de bajas está establecida de la siguiente manera:

- Renuncias
- Muerte
- Jubilación obligatoria (70 años)
- Jubilación voluntaria
- Destitución por sumario administrativo
- Destitución por sanción
- Supresión de puestos por acción de personal
- Supresión de puestos por bonificación
- Agradecimiento de servicio
- Ascenso

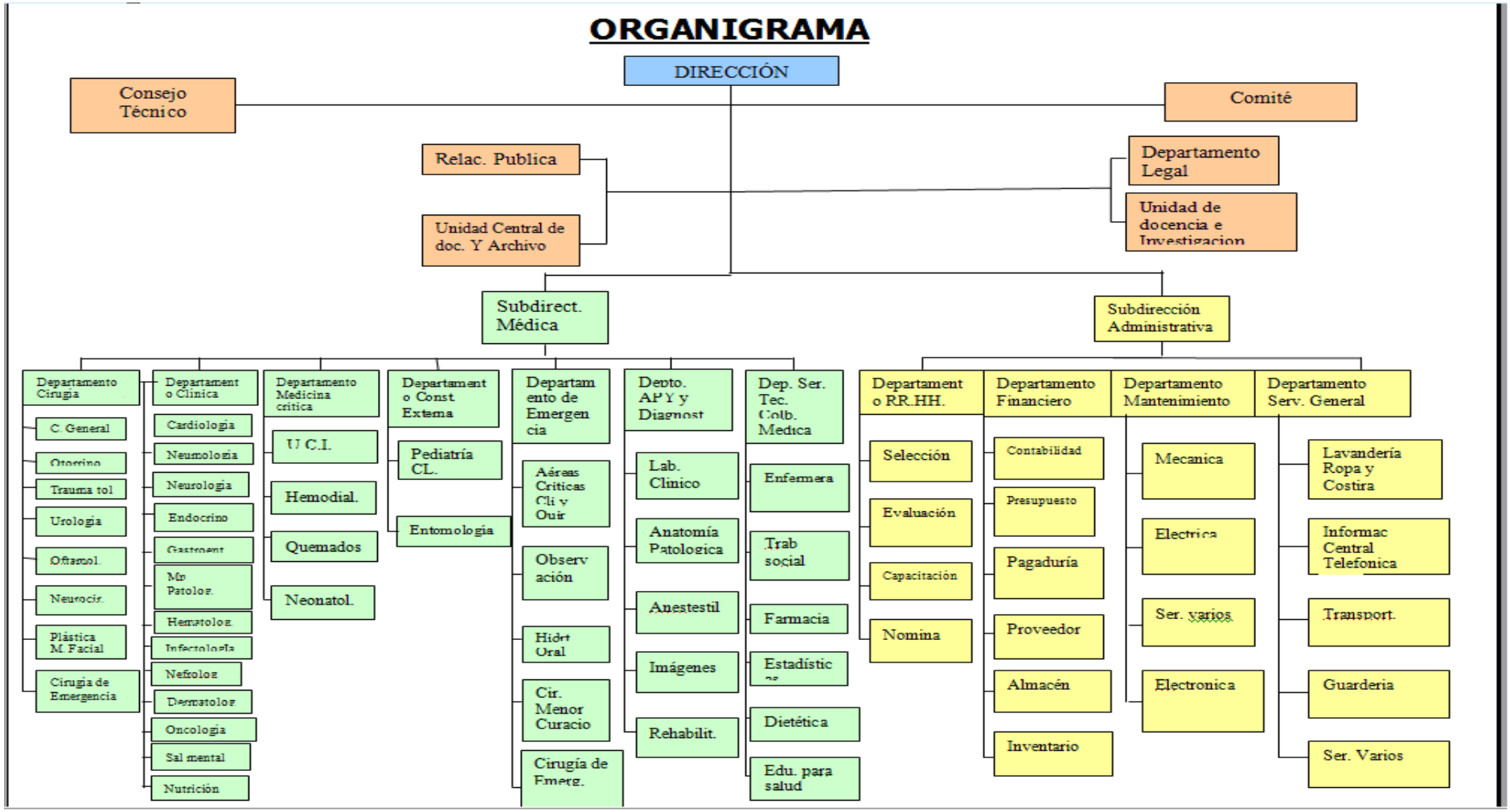


Fig. F.6 Organigrama Hospital de Niños Francisco Icaza Bustamante

CAPÍTULO 3

PLANIFICACIÓN

3 PLANIFICACIÓN

3.1 ALCANCES Y LÍMITES DEL SISTEMA

3.1.1¿Qué es?

Elegir adecuadamente el alcance es de suma importancia a la hora de abordar la implantación de un SGSI; Un alcance excesivo puede hacer un proyecto inabordable y llevarlo al fracaso; un alcance muy reducido puede no contemplar aspectos importantes y dar resultado que no sea útil para los propósitos de la organización.

Para una correcta delimitación del alcance hay que combinar criterios de negocio, criterios organizativos y criterios técnicos

La norma ISO27000 nos define una lista de dominios en los que se debe aplicar la Seguridad de la Información la misma que se encuentra en el ANEXO

En este proyecto de tesis al ser de corto tiempo de duración y sumando además que el Organismo a implantar el SGSI es muy grande de abarcar, hemos tomado la decisión:

El sistema de gestión de seguridad de la información está destinado cubrir toda la información que queda expuesta a sufrir cambios, alteraciones o robo cuando un empleado de la Organización da por terminada la relación laboral o existen una modificación de la misma.

3.1.2Alcance del Sistema planteado al Organismo

El modelo de SGSI orientado al Organismo se aplicará en los siguientes ambientes:

- Recursos humanos al finalizar su relación laboral:
  - Destitución
  - Renuncias
  - Muerte
  - Jubilación
  - Supresión de puestos

El Sistema de Seguridad será lo suficientemente eficaz para proteger la información en el momento en que un empleado cese sus funciones o sean modificadas, bloqueando su acceso y eliminando sus privilegios con respecto a la información exclusiva del Organismo.

3.2 POLÍTICAS DE SEGURIDAD

3.2.1Definición

"Las Políticas son documentos de alto nivel". Ellas representan la filosofía corporativa de una organización y el pensamiento estratégico de la alta gerencia y de los dueños de los procesos del negocio. Las políticas deben ser claras y concisas para que sean efectivas. La administración debe crear un ambiente de control positivo, asumiendo la responsabilidad de formular, desarrollar, documentar, promulgar y controlar las políticas que abarcan las metas y las directrices generales.

3.2.2Consideraciones Generales

Como mínimo, en Recursos Humanos se manejan datos de nivel medio (datos financieros), pero es muy común que el nivel realmente sea el alto: información sobre bajas laborales o discapacidades otorgan al fichero de empleados el nivel alto y convierten al departamento de Recursos Humanos en el de mayor importancia en la protección de datos personales.

La Dirección General del Organismo, a través del Centro de Cómputo facilita a los usuarios el equipamiento informático necesario para la realización de las tareas relacionadas con su puesto de trabajo.

Los equipos y dispositivos de cómputo son bienes del Organismo y el cuidado y buen funcionamiento de estos equipos depende de todos los colaboradores y funcionarios del mismo.

El cuidado del computador y los ambientes computacionales facilitan el normal desarrollo de las actividades cotidianas.

Estas Políticas y Procedimientos serán aplicados en las instalaciones designadas al uso de RRHH. Del Organismo, las mismas que serán reconocidas y acatadas por todos los colaboradores y funcionarios del mismo.

También se involucran a terceros que tengan acceso físico, acceso a cualquier recurso informático o de información sea digital o impresa que sean de propiedad de RRHH del Organismo.

3.2.3 Políticas

PS 1. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

PS 2. En el momento de la contratación será obligado un compromiso por escrito en que se acepta la confidencialidad de cada una de sus labores mantenidas con la organización.

PS 3. Con el fin de mantener la integridad del sistema es estrictamente necesario cumplir las medidas de seguridad establecidas en cada momento.

PS 4. Toda persona que utilice un ordenador en su trabajo habitual deberá identificarse para su uso con un «nombre de usuario», facilitado por el Centro de Cómputo, y una «contraseña», construida por el propio usuario según las normas definidas por dicha centro; las mismas que serán retiradas al usuario en el momento de la baja laboral.

PS 5. Con objeto de mejorar las prestaciones del sistema y ante posibles averías o incidencias se recomienda tener organizados los datos en carpetas y subcarpetas y eliminar los datos innecesarios, sobre todo los que afectan al correo electrónico, los mismos que deberán quedar registrados en el computador al momento del proceso de terminación laboral, para su posible necesidad.

PS 6. Cada usuario será responsable de la integridad de la información almacenada en el ordenador personal que tenga asignado, que dispone de grabador de CD's para facilitar las tareas de salvaguarda, los mismos que quedarán a disposición de la organización.

PS 7. Cada persona que en su momento de contratación haya adquirido una serie de elementos ya sean equipos, archivos, manuales, dispositivos de almacenamiento, etc. estos serán registrados en un inventario de aceptación. Y se ha comprometido por escrito a su total devolución en las mismas condiciones en el momento de su baja laboral.

PS 8. La organización debe ser proactivo en el cumplimiento de la ley y la protección de sus datos, no conviene olvidar que, según el artículo 12 de la LOPD, aunque la gestión de nóminas o trámites legales esté subcontratada, la titularidad de los datos y responsabilidad final no puede ser delegada. Existe la obligación de asegurar que cualquier tercera parte protege la información adecuadamente.

PS 9. Serán de obligada observancia la cautela y el celo profesional en el tratamiento de cualquier tipo de información mecanizada que se gestione en función de las tareas asignadas a cada usuario. Se tendrá especial cuidado con los datos de carácter confidencial.

PS 10. Las historias clínicas de los pacientes, son consideradas como información confidencial entre el paciente y el médico.

PS 11. Las historias clínicas de los pacientes, son de dominio privado, por lo que se prohíbe su uso fuera de las instalaciones del Organismo.

PS 12. Las historias clínicas deben ser de único interés médico, por lo que no compete el uso con fines diferentes.

PS 13. La información del personal del Organismos son de carácter confidencial; dado que no existe aún una ley reguladora que proteja los datos personales se podría acogerse a la institución del Hábeas Data, establecida en el artículo 94 de la Constitución.

3.3 ANÁLISIS DE RIESGOS

3.3.1 ¿Qué es?

El análisis de riesgos es una herramienta que permite identificar, clasificar y valorar los eventos que pueden amenazar la consecución de los objetivos de la Organización y establecer las medidas oportunas para reducir el impacto esperado hasta un nivel aceptable.
El análisis de riesgo puede tener distintos destinatarios dentro de la organización. Cada destinatario necesita esta información para fines distintos, y por ello, necesita recibir la información presentada de forma diferente

3.3.2 Consideración Del Riesgo

El riesgo, en la medida en que supone una exposición potencial a un impacto negativo para el cumplimiento de los objetivos de una Organización, tiene una connotación negativa.

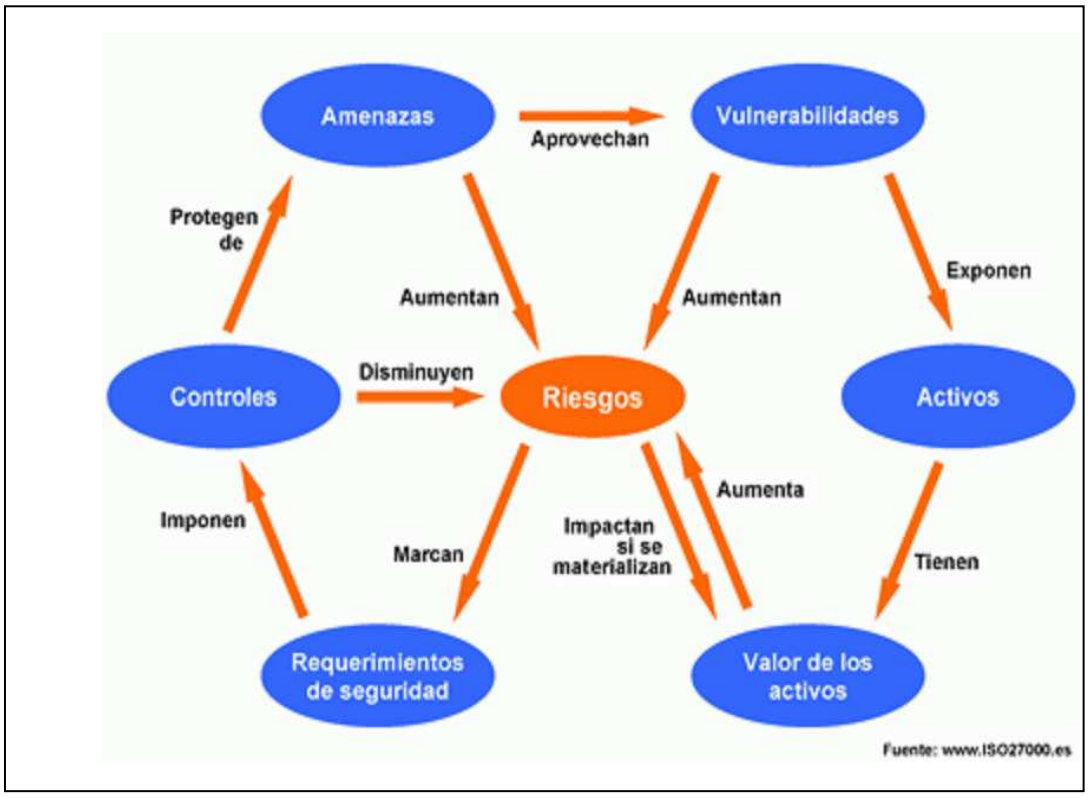


Fig. F.7 Análisis de riegos

3.3.3 Identificación de Activos

3.3.3.1¿Qué es?

Un activo es todo aquello que contiene información que sea de vital importancia para la Organización.

3.3.3.2Tipos de activos

1	SERVICIO
2	DATOS
3	APLICACIONES
4	EQUIPOS INFORMÁTICOS
5	SOPORTE DE INFORMACIÓN
6	EQUIPAMIENTO AUXILIAR
7	INSTALACIONES
8	PERSONAL

Tabla 1.1 Tipos de activos

3.3.3.3Catálogo de Activos

A.00	DATOS
A-01	Base de datos ministerial de empleados
A-02	Base de datos propia de empleados
A-03	Registros de roles
A-04	Registros de IESS
A-05	Registro de inventario asignado
A-06	Archivos vida laboral de empleados
A-07	Archivos de pacientes
E-00	APLICACIONES
E-01	ESIPREN
D-00	PERSONAL
D-01	Director general
D-02	Jefe de áreas administrativas
S-00	EQUIPO IINFORMÁTICO
S-01	CPU
H-00	INSTALACIONES
H-01	Áreas restringidas

Tabla 1.2 Catalogo de activos

3.3.3.4Descripción general de activos

Código: A-01Nombre de Activo: Base de datos ministerial de empleados.

Descripción: Base de datos que registra todos los empleados que prestan sus servicios al Organismo, cubre todos los niveles jerárquicos; incluyen campos de datos de nombre, apellido, documento identidad, código de empleado, fecha de alta, puesto que cubre, ascensos, procesos disciplinarios; es decir, toda la vida laboral que ha tenido dentro de la Organización. Esta base de datos está bajo el dominio del Ministerio de Salud, compartida con el Ministerio de Finanzas y el Organismo el que está a cargo de su mantenimiento, y actualización.

El acceso a la base de datos es a través de conexión internet, el software que se ejecuta para el mantenimiento y la actualización está instalado en solo una máquina del Dpto. de RRHH.

Su acceso a través de la aplicación está asignado a una sola persona del Dpto., la misma que tiene asignado un USER y un PASSWORD, el mismo que es compartido con el Director del Dpto. de RRHH paro su uso en caso de ausencia o algún otro imprevisto.

Los datos pueden ser consultados por el Dpto. de Nómina bajo un USER y un PASSOWRD con acceso de solo lectura.

Código: A-02Nombre de Activo: Base de datos propia de empleados

Descripción: Base de datos de los empleados del Organismo; cubre todas las áreas y todos los niveles jerárquicos. El acceso está controlado con USER y PASSORD, los mismos que son de poca confidencialidad entre los empleados del Dpto. Su uso es de poca utilidad ya que solo es a nivel de consulta, ya sea de puesto a cargo, años de antigüedad, jefe inmediato u área de trabajo. Su modificación no es de asignación específica dentro de los empleados del área de RRHH. el cual puede ser ejecutado por cualquiera que lo necesite.

Código: A-03Nombre del Activo: Registro de Roles

Descripción: Los Roles de pago de cada empleado son almacenados en hojas de cálculo (Excel) los mismos que son guardados en el servidor, su acceso se permite exclusivamente al Departamento de Roles de Pago, pero la información que contiene no es de uso exclusivo del Dpto. ya que se puede visualizar de muchísimas formas, ya que aún no conciben la idea de que es información confidencial, que compete únicamente al empleado. Por ejemplo, al firmar el recibido del rol de pago, se entrega al empleado un listado donde están registrados los empleados en orden alfabético con nombre, cargo, sueldo, descuentos y datos adicionales, que pueden ser leídos con total libertad.

Código: A-05Nombre del activo: Registro de inventario asignado

Descripción: En el momento de ingreso de un empleado, o en el cambio de funciones, según sea el caso; dependiendo de su nivel jerárquico, se le puede o no asignar el uso y la responsabilidad de ciertos equipos con los que podrá realizar sus funciones, sean estos de carácter técnicos, médicos, informáticos o de cualquier otro nivel, estos quedan asentados en un registro de inventario asignado, el mismo que puede ser consultado previa petición al encargado de inventarios sin que sea necesario mayor control de acceso a dicha información.

Código: A-06Nombre del activo: Archivos vida laboral de empleados

Descripción: Cada empleado tiene asignado un folder, en el que contiene cada una de las actividades que van surgiendo en el cumplimiento de sus funciones, como por ejemplo los memorándum enviados, las vacaciones disfrutadas, los ascensos, las sanciones recibidas y demás; estos folders a su vez son contenidos dentro de archivadores que se encuentran en una pequeña área perteneciente al Dpto. de RRHH. y que son resguardados por una puerta de acceso con llave de seguridad, la misma que se encuentra bajo el resguardo de una persona a cargo, pero que son guardadas dentro del Dpto. al alcance de cualquier necesidad. Estos documentos son originales sin copia que están sin ningún sistema de seguridad, llámese a estos: detector de humo, detector de incendio, alarma, e incluso impermeabilización del área.

Código: A-07Nombre del activo: Archivos de pacientes

Descripción: En el primer momento que un infante tiene contacto con el Organismo, se crea una carpeta con un código asignado al que le llamarán historia clínica. En esta carpeta se registra y almacena cada una de las citas realizadas por el menor así como los diagnósticos y tratamientos que han suscitado como también las pruebas médicas solicitadas con sus respectivos desgloses de información.

Estas carpetas son almacenadas dentro del Dpto. de Estadística, y en el momento que el paciente regresa a consulta, la carpeta es retirada de su lugar, para ser enviada al médico asignado. Generalmente las carpetas de cada médico son trasladadas por personal destinado a esas funciones, aunque se crean situaciones en las que el médico tiene la necesidad de solicitar la carpeta de su paciente a través de personal ajeno a estas funciones, los mismos que pueden retirar la carpeta del Dpto. de Estadística sin ningún control o medida de seguridad que justifique la salida de documentación privada de los pacientes. Permitiendo incluso que la documentación salga de los límites de la Organización sin motivos concretos.

Código: E-01Nombre del Activo: Esipren

Descripción: Este software sirve para trabajar conjuntamente con el Ministerio de Salud, está instalado en una sola máquina del Dpto. de RRHH. Solo una persona tiene acceso con un USER y PASWORD a todos los procesos que contiene. El USER y PASWORD es compartido con el jefe del departamento. Este software es utilizado para el registro de alta de cada empleado, consulta de roles, consulta de la vida laboral de cada empleado; al momento del cese del empleo, es dado de baja a través del software, registrándose en la base de datos del Ministerio de Finanzas y de Salud la desvinculación del mismo con el Organismo. Es decir, todo proceso, modificación o registro que se haga desde el software, se verá reflejado ambos Ministerios.

Código: H-01Nombre del activo: Áreas restringidas

Descripción: Existen áreas en las que se manejan información confidencial, tanto del paciente como del personal que labora en la Organización; lugares como Caja donde se entregan los roles dejando el libre acceso de la información de cada empleado; el área destinado a los archivadores de la vida laboral de cada empleado; el área de estadística donde se archivan las carpetas de las historias clínicas de cada paciente; el área de centro de cómputo que no cuenta con un bloqueo en la puerta de acceso que limite el paso a personas ajenas al mismo. En general, el Organismo no ha transmitido durante todos estos años de función, la necesidad del resguardo de cada información que maneja, dejando los accesos físicos de las áreas a libre disposición del personal.

Código: D-01Nombre del activo: Director General

Descripción: El cargo desempeña muchas obligaciones, responsabilidades y derechos para poder realizar todas las funciones necesarias en el buen manejo de las diversas situaciones que acontecen dentro del Organismo. Es así que cada cambio de dirección que ha tenido el Organismo ha necesitado un periodo de adaptación y ubicación para poder continuar con las funciones; esto se debe a todo el conocimiento y experiencia acumulada que día a día se necesita para poder afrontar el cargo, conocimiento que no se deja plasmado en un documento y que deja un vacío notorio en cada proceso de cambio, es obligación urgente para cada nuevo Director, el ponerse al día en los caminos y procesos establecidos que no están registrados en ninguna parte, experiencia que toca volver a vivirlas para poder tener planteado los pasos a seguir en algunas situaciones que no son nuevas dentro del Organismo.

Código: D-02Nombre del activo: Jefe de áreas

Descripción: El cargo de jefe es asignado al empleado que por méritos y experiencia está plenamente capacitado; pero al igual que cualquier ascenso el cambio de funciones que necesita un periodo de adaptación, procedimientos que necesitan

cambios, procesos que mejoran, problemas que buscan otra vía de solución, etc. Experiencia que se acumula día a día y que queda registrado solamente en quien ocupa el cargo y no en el cargo específicamente. Por lo que es notorio la falta de documentación que ayude a la resolución de problemas ya vividos, y que necesitan ser re-planteados en busca de soluciones. Es esa información que posee quien ocupa el cargo, que es necesaria para la continuidad de las funciones.

3.4 AMENAZAS DE LOS ACTIVOS

3.4.1¿Qué es?

Llámese amenaza a una declaración intencionada para hacer un daño, como por ejemplo mediante un virus, un acceso no autorizado o robo.

Pero no se debe pensar que únicamente personas pueden ser los causantes de estos daños, pues existen otros factores como las causas naturales, que son capaces de desencadenar daños materiales o pérdidas inmateriales en los activos, y son también consideradas como amenazas.

Una vez identificados los procesos involucrados en la gestión de clientes, el siguiente paso es identificar las principales amenazas que pueden afectar a los activos de información. Las amenazas pueden tener un origen natural o humano, y pueden ser accidentales o deliberadas.

Amenazas del entorno:
Las amenazas generadas por el entorno pueden ser catástrofes naturales (inundaciones, tormentas, terremotos, etc.), acciones de origen humano intencionadas (posibles robos, asaltos, errores técnicos, etc.), o accidentales como el corte del suministro eléctrico.

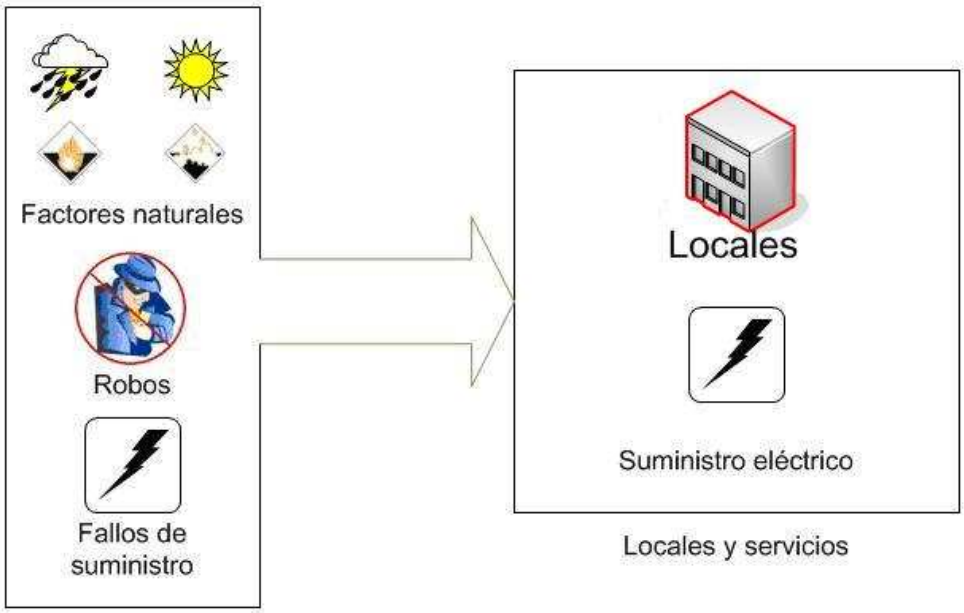


Fig. F.8 Amenazas de entorno

Amenazas propias del sistema de información:

Las principales amenazas que pueden sufrir los sistemas de información son las que afectan a alguno de los elementos que lo forman o explotan. Podemos distinguir tres grupos:

- hardware

- software

- personal que utiliza cualquiera de los dos recursos anteriores.

En los equipos físicos del sistema de información (servidores, equipos informáticos y hardware de comunicaciones), existen amenazas debidas a errores de uso o mantenimiento, y a fallos o averías de cualquiera de sus componentes.

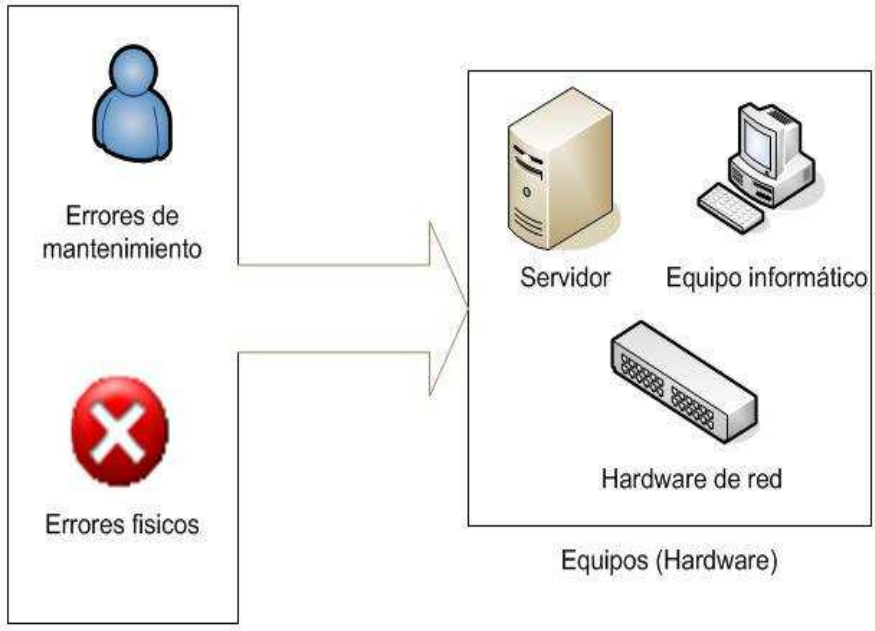


Fig. F.9 Amenazas del sistema

En relación al software de tratamiento de la información (sistema operativos, aplicaciones de negocio, ofimática, etc.) las principales amenazas pueden ser fallos en programación (que permitan la existencia de puertas traseras, errores en la realización de cálculos, etc.), y código malicioso como son los virus informáticos, gusanos, troyanos, etc.

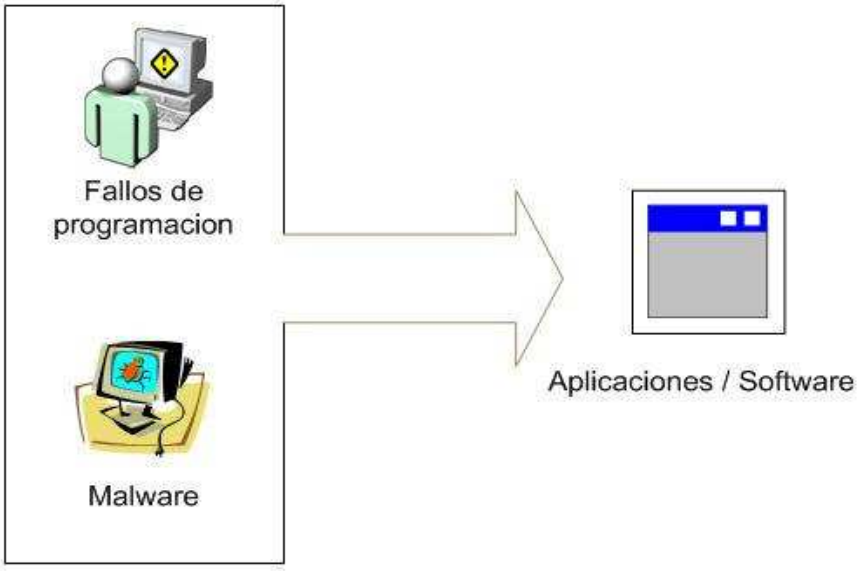


Fig. F.10 Fallos de software

Respecto al uso que realiza el personal de la empresa en el desarrollo de la gestión del pedido, las posibles amenazas son: errores no intencionados -como el borrado accidental de información o la mala introducción de datos- y amenazas de origen intencionado, como posibles robos o filtraciones de información.

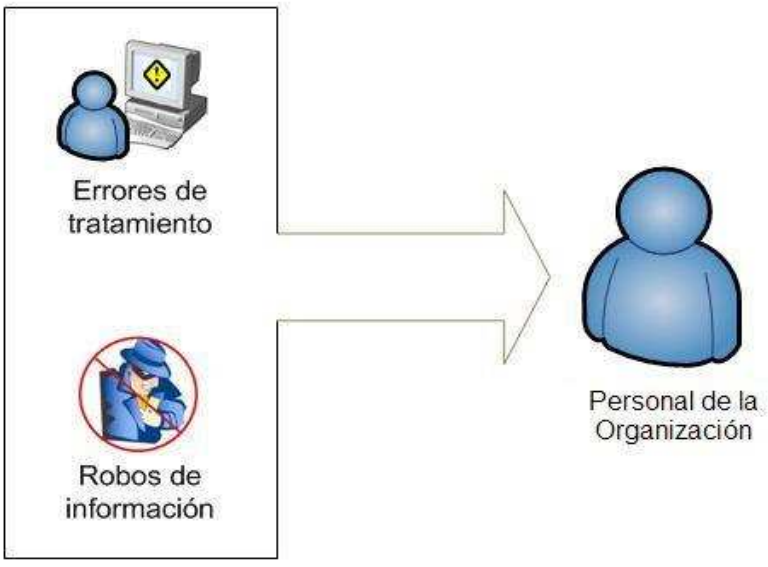


Fig. F.11 Errores del personal

3.4.2 Valoración de Activos

Los activos serán puntuados dependiendo de una tabla de ponderaciones en las que se evalúa la disponibilidad, integridad, confidencialidad de cada uno de los activos. Al obtener cada uno de los puntajes asignados estos se promedian para poder obtener la valoración final de cada uno, dato que nos servirá para calcular el nivel de riesgo.
VALOR = PROM (DISPONIBILIDAD+INTEGRIDAD+CONFIABILIDAD)

PUNTUACIÓN	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
5	siempre	extrema	uso confidencial
4	exenta por horas	importante	uso restringido
3	exenta por 24h	media	semi-restringido
2	exenta por 48h	no importante	uso interno
1	exenta varios días	insignificante	acceso público

Tabla 1.3 Escala de puntuaciones de valores de los activos

3.4.3Valoración de Activos

A.00	DATOS	Disp.	Integridad	Confid.	VALOR
A-01	Base de datos ministerial de empleados	5	5	5	5
A-02	Base de datos propia de empleados	4	5	5	5
A-03	Registros de roles	5	5	4	5
A-04	Registros de IESS	5	5	4	5
A-05	Registro de inventario asignado	4	5	1	3
A-06	Archivos vida laboral de empleados	5	5	4	5
A-07	Archivos de pacientes	5	5	5	5
E-00	APLICACIONES	Disp.	Integridad	Confid.	VALOR
E-01	ESIPREN	5	5	4	5
D-00	PERSONAL	Disp.	Integridad	Confid.	VALOR
D-01	Director general	4	5	5	5
D-02	Jefe de áreas administrativas	4	4	5	4
S-00	EQUIPO INFORMÁTICO	Disp.	Integridad	Confid.	VALOR
S-01	Punto de acceso (CPU)	3	5	3	4
H-00	INSTALACIONES	Disp.	Integridad	Confid.	VALOR
H-01	Áreas restringidas	5	5	5	5

Tabla 1.4 Asignación de valores a los activos

3.4.4TABLAS DE PUNTUACIÓN DEL ANÁLISIS DE RIESGO

DEGRADACIÓN DEL ACTIVO (si la falla ocurre)	
Descripción	**Degradación %**
Baja	25
Media	50
Alta	75
Total	100

Tabla 1.5 Ponderación de Degradación

VALORACIÓN DE FALLAS		
Prob. de Ocurrencia	**Descripción**	**Valor**
Extrema	más de 1 vez por semana	6
Muy Alta	1 vez por semana como máximo	5
Alta	1 vez al mes como máximo	4
Media	De 2 a 3 veces por año	3
Baja	1 vez al año como máximo	2
Muy Baja	2 a 3 veces cada 5 años	1
Remota	Muy poco probable que ocurra	0

Tabla 1.6 Ponderación de Ocurrencias

VALORACIÓN DE LA GESTIÓN		
Probabilidad de Gestión	**Descripción**	**Valor**
Muy Baja	Muy Difícil de Detectar o Corregir.	5
Baja	Difícil de Detectar o Corregir.	4
Media	Con esfuerzo para Detectar y Corregir	3
Alta	Fácil de Detectar pero con Esfuerzo para Corregir	2
Muy Alta	Muy fácil de Detectar y Corregir	1

Tabla 1.7 Ponderación de Gestión

Realizaremos el cálculo del análisis de riesgos, habiendo obtenido las ponderaciones anteriores dependiendo de cada activo; el valor de riesgo de cada activo se obtiene:

RIESGO = VALOR * DEGRADACIÓN * OCURRENCIA

Con el valor del riego de cada uno de los activos deberemos evaluar la capacidad de las políticas establecidas para detectar cada una de las amenazas cuando afectan al activo; el valor NPR es el que finalmente evaluaremos para clasificar los riesgos a los que deberían aplicarse controles

NPR = RIESGO * PROB DE GESTIÓN

3.5 HOJA DE CÁLCULO DE ANÁLISIS DE RIESGOS

CÓDIGO ACTIVO	VALOR	AMENAZA	DEGRADACIÓN	PROB. DE FALLA	NIVEL DE RIESGOS	CONTR ACTUAL	VAL. DE LA GESTIÓN	NPR ACTUAL
A-01	5	Alteración de la Información	100%	1	5	EXISTE	3	15
A-01	5	Introducción de inf. Incorrecta	100%	1	5	EXISTE	2	25
A-01	5	Destrucción de la Información	75%	1	4	EXISTE	4	16
A-01	5	Divulgación de La información	75%	1	4	EXISTE	5	20
A-01	5	Manipulación de la Configur.	75%	1	4	EXISTE	3	12
A-01	5	Acceso no Autorizado	75%	1	4	EXISTE	4	16
A-01	5	Interceptación de Información	75%	1	4	EXISTE	5	20
A-01	5	Corrupción de la información	75%	1	4	EXISTE	5	20
A-02	5	Alteración de la Información	100%	1	5	NO EXISTE	4	20
A-02	5	Introducción de inf. Incorrecta	100%	2	10	NO EXISTE	2	20
A-02	5	Destrucción de la Información	100%	1	5	NO EXISTE	3	15
A-02	5	Divulgación de La información	50%	5	13	NO EXISTE	5	65
A-02	5	Manipulación de la Configur.	50%	2	5	NO EXISTE	2	10
A-02	5	Acceso no Autorizado	100%	5	25	NO EXISTE	5	125
A-02	5	Corrupción de la información	50%	2	5	NO EXISTE	5	25
A-03	5	Alteración de la Información	100%	1	5	EXISTE	2	10
A-03	5	Introducción de inf. Incorrecta	100%	1	5	EXISTE	2	10
A-03	5	Destrucción de la Información	75%	1	4	EXISTE	2	8
A-03	5	Divulgación de La información	25%	4	5	NO EXISTE	5	25
A-03	5	Manipulación de la Configur.	100%	1	5	EXISTE	3	15
A-03	5	Acceso no Autorizado	100%	1	5	NO EXISTE	4	20
A-03	5	Interceptación de Información	25%	3	4	NO EXISTE	5	20
A-03	5	Corrupción de la información	25%	3	4	EXISTE	2	8
A-04	5	Alteración de la Información	100%	1	5	EXISTE	2	10
A-04	5	Introducción de inf. Incorrecta	100%	1	5	EXISTE	4	20
A-04	5	Destrucción de la Información	75%	1	4	EXISTE	4	16
A-04	5	Divulgación de la Información	50%	3	8	NO EXISTE	5	40
A-04	5	Manipulación de la Información.	100%	1	5	EXISTE	2	10

A-04	5	Acceso no Autorizado	50%	2	5	NO EXISTE	5	25
A-04	5	Interceptación de Información	50%	3	8	EXISTE	3	24
A-05	5	Alteración de la Información	100%	2	10	NO EXISTE	3	30
A-05	5	Introducción de inf. Incorrecta	100%	2	10	NO EXISTE	4	40
A-05	5	Destrucción de la Información	100%	1	5	NO EXISTE	4	20
A-05	5	Divulgación de la Información	25%	3	4	NO EXISTE	4	16
A-05	5	Manipulación de la Información.	25%	1	1	NO EXISTE	2	2
A-05	5	Acceso no Autorizado	25%	3	4	NO EXISTE	4	16
A-05	5	Interceptación de Información	25%	3	4	NO EXISTE	4	16
A-06	5	Alteración de la Información	100%	2	10	NO EXISTE	3	30
A-06	5	Introducción de inf. Incorrecta	100%	3	15	NO EXISTE	3	45
A-06	5	Destrucción de la Información	100%	1	5	NO EXISTE	5	15
A-06	5	Divulgación de la Información	50%	5	13	NO EXISTE	5	65
A-06	5	Manipulación de la Información.	50%	1	3	NO EXISTE	3	9
A-06	5	Acceso no Autorizado	50%	5	13	NO EXISTE	2	26
A-06	5	Interceptación de Información	50%	5	13	NO EXISTE	5	65
A-07	5	Alteración de la Información	100%	2	10	NO EXISTE	5	50
A-07	5	Introducción de inf. Incorrecta	100%	2	10	NO EXISTE	5	50
A-07	5	Destrucción de la Información	100%	1	5	NO EXISTE	5	25

A-07	5	Divulgación de la Información	50%	5	13	NO EXISTE	5	65
A-07	5	Manipulación de la Información.	50%	5	13	NO EXISTE	5	65
A-07	5	Acceso no Autorizado	50%	5	13	NO EXISTE	5	65
A-07	5	Interceptación de Información	50%	5	13	NO EXISTE	5	65
E-01	5	Errores de Usuario	25%	1	1	EXISTE	1	1
E-01	5	Errores de Administrador	25%	1	1	EXISTE	1	1
E-01	5	Errores de Configuración	50%	1	3	EXISTE	2	6
E-01	5	Escape de Información	25%	1	1	EXISTE	4	4
E-01	5	Vulnerabilidad de los Programas	50%	1	3	EXISTE	3	9
E-01	5	Caída Del Sistema	50%	2	5	EXISTE	1	5
E-01	5	Error en Act. de Programas	100%	1	5	EXISTE	1	5
E-01	5	Manipulación de la Configur.	100%	1	5	EXISTE	2	10
E-01	5	Suplantac. de Ident. de Usuario	50%	1	3	EXISTE	3	9
E-01	5	Abuso de Privilegios de Acceso	75%	1	4	EXISTE	3	12
E-01	5	Uso no Previsto	50%	1	3	EXISTE	4	12
E-01	5	Difusión de Software dañino	100%	1	5	EXISTE	2	10
E-01	5	Acceso no Autorizado	25%	1	1	EXISTE	2	2

E-01	5	Interceptación de Información	50%	2	5	EXISTE	3	15
E-01	5	Manipulación de Programas	75%	1	4	EXISTE	2	8
E-01	5	Indisponibilidad del personal	75%	2	8	EXISTE	1	8
S-01	4	Abuso de Privilegios de Acceso	50%	2	4	NO EXISTE	5	20
S-01	4	Uso Indebido	50%	5	10	NO EXISTE	5	50
S-01	4	Acceso no Autorizado	50%	1	2	NO EXISTE	4	8
S-01	4	Interceptación de Información	50%	1	2	NO EXISTE	4	8
S-01	4	Robo	100%	1	4	NO EXISTE	2	8
D-01	5	Deficiencias en la organización	100%	3	15	NO EXISTE	3	45
D-01	5	Indisponibilidad del personal	50%	2	5	NO EXISTE	1	5
D-01	5	Extorsión	100%	1	5	NO EXISTE	4	20
D-02	5	Deficiencias en la organización	100%	3	15	NO EXISTE	3	45
D-02	5	Indisponibilidad del personal	50%	2	5	NO EXISTE	1	5
D-02	5	Extorsión	100%	1	5	NO EXISTE	4	20
D-02	5	Segregación responsabilidades	100%	4	20	NO EXISTE	4	80
H-01	5	Uso no Previsto	50%	4	10	NO EXISTE	5	50
H-01	5	Acceso no Autorizado	75%	4	15	NO EXISTE	5	75

Tabla 1.8 Análisis de Riesgo

3.5.1 Nivel de riesgos

La metodología nos indica que existen riesgos que son asumibles por la empresa, riesgos de nivel bajo, riesgos de nivel medio y riesgos de alto nivel. A estos 2 últimos serán a los que le plantearemos controles para poder reducirlos a un nivel bajo, o asumible en mejor de los casos.
Para esto existe una tabla de ponderaciones:

NIVEL	*ESCALA*
ALTO	**61-125**
MEDIO	**36-60**
BAJO	**24-35**
ASUMIDO	**0-23**

Tabla 1.9 Escala de los ponderaciones de riesgos

Resumen

Dada la tabla de ponderación de los valores según la escala establecida, extraemos el siguiente resumen de todas las amenazas que hemos encontrado en el funcionamiento de las etapas de nuestro alcance.

GRADO DE RIESGO	AMENAZAS
Rojos	10
Amarillo	9
Verdes	9
Gris	53

Tabla 1.10 Riesgos encontrados en el Organismo

3.6 TRATAMIENTO DE RIESGO

CÓDIGO	ACTIVO	AMENAZA	VALOR	DEGRADAC.	PROB. DE FALLA	NIVEL DE RIESGO	CONTROL ACTUAL	VAL. DE LA GESTIÓN	NPR ACTUAL	TRATAMIENTO DE RIESGO
A-02	Base de datos propia empleados	Divulgación de La información	5	50%	5	13	NO EXISTE	5	65	Mitigar
A-02	Base de datos propia empleados	Acceso no Autorizado	5	100%	5	2	NO EXISTE	5	125	Mitigar
A-04	Registro del IESS	Divulgación de La información	5	50%	3	8	NO EXISTE	5	40	Mitigar
A-05	Registro de inventario asignado	Introducción de inf. Incorrecta	5	100%	2	10	NO EXISTE	4	40	Eliminar
A-06	Archivos vida laboral de empleados	Introducción de inf. Incorrecta	5	100%	3	15	NO EXISTE	3	45	Eliminar
A-06	Archivos vida laboral de empleados	Divulgación de La información	5	50%	5	13	NO EXISTE	5	65	Mitigar
A-06	Archivos vida laboral de empleados	Interceptación de información	5	50%	5	13	NO EXISTE	5	65	Mitigar
A-07	Archivos de pacientes	Alteración de la información	5	100%	2	10	NO EXISTE	5	50	Eliminar
A-07	Archivos de pacientes	Introducción de inf. Incorrecta	5	100%	2	10	NO EXISTE	5	50	Mitigar
A-07	Archivos de pacientes	Divulgación de La información	5	50%	5	13	NO EXISTE	5	65	Mitigar
A-07	Archivos de pacientes	Manipulación de la Configur.	5	50%	5	13	NO EXISTE	5	65	Eliminar
A-07	Archivos de pacientes	Acceso no Autorizado	5	50%	5	13	NO EXISTE	5	65	Eliminar
A-07	Archivos de pacientes	Interceptación de información	5	50%	5	13	NO EXISTE	5	65	Mitigar
S-01	Punto de acceso(CPU)	Uso no Previsto	4	50%	5	10	NO EXISTE	5	50	Mitigar
D-01	Director general	Deficiencias en la organización	5	100%	3	15	NO EXISTE	3	45	Mitigar
D-02	Jefes de áreas administrativas	Deficiencias en la organización	5	100%	3	15	NO EXISTE	3	45	Mitigar
D-02	Jefes de áreas administrativas	Segregación de responsabilidad	5	100%	4	20	NO EXISTE	4	80	Eliminar
H-01	Áreas restringidas	Acceso no Autorizado	5	75%	4	15	NO EXISTE	5	75	Mitigar
H-01	Áreas restringidas	Uso no Previsto	5	50%	4	10	NO EXISTE	5	50	Mitigar

Tabla 1.11 Tratamiento de Riesgo

3.7 DOCUMENTO DE APLICABILIDAD S O A

OC: Obligaciones Contractuales-; RN/ABP: Requisitos de Negocio/Adopción de Buenas Prácticas-; RER: Resultados de Evaluación de Riesgo

Controles ISO 27001:2005			Control Excluido	Control Actual	Controles Seleccionados y su Justificación				Comentario
					RL	OC	RN/ABP	RER	
Cláusula	#	Objetivo de control							
	8.3	Finalización/cambio del puesto							
SEGURIDAD EN	8.3.1	Cese de responsabilidades					■	■	Todo cargo de alto nivel deberá tener sus funciones y responsabilidades documentadas y con un backup para la continuidad del servicio.
RECURSOS	8.3.2	Restitución de activos				■	■	■	Todo cargo al que se le haya asignado información, equipos o soportes de información, deberán ser registrados por escrito para su devolución.
HUMANOS	8.3.3	Cancelación de permisos de acceso					■	■	A toda persona que quede desvinculada total o parcialmente de las actividades de la organización, se le deberán bloquear o controlar sus accesos.

Tabla 1.12 Documento de Aplicabilidad

CAPÍTULO 4

ETAPA DO

4 ETAPA DO

4.1 NORMATIVAS DE CONTROLES DE PERSONAL

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.

Atendiendo al principio de que "la cadena es tan fuerte como el más débil de sus eslabones", en toda organización se cumple que el eslabón más débil es el personal.

Antes de establecer los controles específicos a cada una de las amenazas encontradas en el sistema que ha venido funcionando en el Organismo, debemos poner en conocimiento ciertos términos que se verán reflejados en el planteamiento de los controles:

4.1.1Definición de Funciones y Responsabilidades

Una de las principales amenazas de toda organización 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.

4.1.1.1 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, un depositario 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.

- Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas.
- 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 ISO17799:2005)

4.1.2 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.

4.1.2.1 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.

4.1.2.2 Normativa

La confidencialidad del personal con acceso a datos está regulada, tanto en la Ley de Protección de datos como en la norma ISO 17799.

4.1.3 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 la organización 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.

4.1.3.1 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.

4.1.3.2 Normativa

La regulación sobre la formación y concienciación del personal con acceso a datos está regulada, tanto en la Ley de Protección de datos como en la ISO 17799, en los siguientes puntos:

- La organización deberá identificar y revisar las necesidades de confidencialidad y recogerlas en acuerdos de no divulgación. (Punto 6.1.5 ISO17799:2005)

4.1.4 Responsabilidad en el uso de contraseñas

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.

4.1.4.1 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.

4.1.4.2 Normativa

Las medidas sobre la responsabilidad de los usuarios en el uso de sus contraseñas están reguladas, tanto en la Ley de Protección de datos como en la ISO 17799, 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 17799:2005)

- Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible. (Artículo 11.3 RMS)

- Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. (Artículo 18.2 RMS)

- La asignación de contraseñas debería ser controlada por un proceso de dirección formal. (Punto 11.2.3 ISO17799:2005)

- 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 ISO17799:2005)

4.2 PROCEDIMIENTO

En esta etapa, se propondrá los controles o políticas de seguridad que se establecerán en el Organismo, con el fin de corregir o mitigar aquellas amenazas que atacan directamente a los activos de mayor importancia del Organismo.

Las Políticas de Seguridad que están dentro de nuestro ámbito, se plantean conjuntamente con el procedimiento a seguir para poder llevarlas a cabo. Aquellas que están fuera de nuestro ámbito solo se dejaran planteadas.

4.3 ACTIVO: A02 BASE DE DATOS PROPIA DE EMPLEADOS

4.3.1 Amenaza: Divulgación de la información

Control 8.1.3 Términos y condiciones del empleo
Recomendación
La empresa debe establecer un acuerdo de confidencialidad al momento de firmar el contrato laboral; en el mismo se debe manifestar la ***no divulgación*** de toda información personal en lo que a empleados se refiere y a la de único interés y de uso exclusivo del Organismo.

Política de seguridad

-Todo empleado que inicie su relación laboral con el Organismo, firmará un documento llamado de ***confidencialidad*** que será entregado por RRHH en el momento de la contratación, el mismo que está obligado a cumplir en un periodo de 3 meses después de concluida dicha relación.

Procedimiento

a. El Departamento legal, en conjunto con RRHH y la Dirección del Hospital redactarán un documento de ***confidencialidad***; en el que se obliga al empleado a la no divulgación, ni exposición de toda información que incluya datos de uso exclusivo del Organismo.
b. Este documento deberá ser firmado por cada uno de los empleados en el momento de la contratación.
c. El documento de confidencialidad tendrá vigencia de 3 meses adicionales una vez concluida la relación laboral Empleado-Organismo.

Control 8.3.1 Responsabilidades de terminación
Política de Seguridad

- Una vez que el ex empleado cese sus funciones dentro de la Organización, está obligado a cumplir con la no divulgación de la información de uso exclusivo del Organismo

Procedimiento

a. Cuando un empleado cese sus funciones o el empleado cambie de funciones dentro de la organización, está obligado a cumplir con el acuerdo de confidencialidad; es decir a la no divulgación de la información durante un periodo de 3 meses finalizado el contrato.

4.3.2 Amenaza: Acceso no autorizado

Control 8.3.3 Retiro de los derechos de acceso
Política de Seguridad

-Cuando un empleado cambia su situación laboral, el acceso que este tiene a la información será inhabilitado 24 horas antes de la entrega del documento de acción de personal en el que se comunica el cese o cambio de sus funciones dentro del Organismo; y 24 horas después en caso de renuncia voluntaria sin previo aviso.

-Los derechos de acceso que deberían ser retirados o adaptados incluyen accesos físicos y lógicos, claves, tarjetas de identificación, recursos de tratamiento de la información, suscripciones, así como la retirada de cualquier documentación que les identifique como un miembro actual de la organización.

Procedimiento

a. En caso de renuncia voluntaria, despido forzado, del área de RRHH emitirá la acción de personal (anexo II), en el que se especifica los motivos por el cual el empleado es despedido o procede al cambio de sus funciones.
b. Si el empleado pertenece a alguna de las áreas administrativas en las que se tiene acceso a la información digital, se enviará una copia del documento al Centro de Cómputo para la verificación y posterior inhabilitación de los accesos en caso de los que tuviere del empleado.
c. Si el empleado pertenece a alguna de las áreas administrativas en las que se tiene acceso a las áreas restringidas, el jefe inmediato comunicará la retirada de la tarjeta de acceso o la anulación del registro dactilar dependiendo de la infraestructura instalada.
d. En caso de cambio de sus funciones, un asistente del centro de cómputo y el jefe de la próxima área del empleado, plantearán las modificaciones de los accesos que necesitará para el desarrollo de las obligaciones establecidas.

Control: 9.1.3 Seguridad de oficinas, despachos e instalaciones
Recomendación

Se recomienda que en el archivo de RRHH se instalen seguridades tales como puertas de acceso controladas con tarjetas o con identificadores de huellas dactilares; de esta forma poder proteger aquella área donde se archivan cada una de las carpetas con la vida laboral de cada uno de los empleados.

Política de Seguridad

-El acceso a áreas restringidas será controlado mediante puertas con apertura de lector dactilar.
-El área de archivo de RRHH será considerado como área de acceso restringido

4.4 ACTIVO: A04 REGISTROS DEL IESS

4.4.1 Amenaza: Divulgación de la información

Control 8.1.3 Términos y condiciones del empleo
Recomendación
La empresa debe establecer un acuerdo de confidencialidad al momento de firmar el contrato laboral; en el mismo se debe manifestar la ***no divulgación*** de toda información personal en lo que a empleados se refiere y a la de único interés y de uso exclusivo del Organismo.

Política de seguridad

-Todo empleado que inicie su relación laboral con el Organismo, firmará un documento llamado de ***confidencialidad*** que será entregado por RRHH en el momento de la contratación, el mismo que está obligado a cumplir en un periodo de 3 meses después de concluida dicha relación.

Procedimiento

a. El Departamento legal, en conjunto con RRHH y la Dirección del Hospital redactarán un documento de ***confidencialidad***; en el que se obliga al empleado a la no divulgación, ni exposición de toda información que incluya datos de uso exclusivo del Organismo.
b. Este documento deberá ser firmado por cada uno de los empleados en el momento de la contratación.
c. El documento de confidencialidad tendrá vigencia de 3 meses adicionales una vez concluida la relación laboral Empleado-Organismo.

Control 8.3.1 Responsabilidades de terminación
Política de Seguridad

- Una vez que el ex empleado cese sus funciones dentro de la Organización, está obligado a cumplir con la no divulgación de la información de uso exclusivo del Organismo

Procedimiento
Cuando un empleado cese sus funciones o el empleado cambie de funciones dentro de la organización, está obligado a cumplir con el acuerdo de confidencialidad; es decir a la no divulgación de la información durante un periodo de 3 meses finalizado el contrato.

Control 8.3.3 Retiro de los derechos de acceso
Política de Seguridad

-Cuando un empleado cambia su situación laboral, el acceso que este tiene a la información será inhabilitado 24 horas antes de la entrega del documento de acción de personal en el que se comunica el cese o cambio de sus funciones dentro del Organismo; y 24 horas después en caso de renuncia voluntaria sin previo aviso.

-Los derechos de acceso que deberían ser retirados o adaptados incluyen accesos físicos y lógicos, claves, tarjetas de identificación, recursos de tratamiento de la información, suscripciones, así como la retirada de cualquier documentación que les identifique como un miembro actual de la organización.

Procedimiento

a. En caso de renuncia voluntaria, despido forzado, del área de RRHH emitirá la ***acción de personal*** (anexo II), en el que se especifica los motivos por el cual el empleado es despedido o procede al cambio de sus funciones.
b. Si el empleado pertenece a alguna de las áreas administrativas en las que se tiene acceso a la información digital, se enviará una copia del documento al Centro de Cómputo para la verificación y posterior inhabilitación de los accesos en caso de los que tuviere del empleado.
c. Si el empleado pertenece a alguna de las áreas administrativas en las que se tiene acceso a las áreas restringidas, el jefe inmediato comunicará la retirada de la tarjeta de acceso o la anulación del registro dactilar dependiendo de la infraestructura instalada.

a. En caso de cambio de sus funciones, un asistente del centro de cómputo y el jefe de la próxima área del empleado, plantearán las modificaciones de los accesos que necesitará para el desarrollo de las obligaciones establecidas.

4.5 ACTIVO: A-05 REGISTRO DE INVENTARIO ASIGNADO

4.5.1 Amenaza: Introducción de información incorrecta

Política de Seguridad

-El control de inventario de activos se realizará cada tres meses, en el cual cada empleado deberá confirmar los activos asignados al inicio de sus funciones.

Procedimiento

a. El jefe del área de inventario planificará el control de activos presentando un cronograma al Director general, proponiendo la fecha para el inicio del mismo; cronograma que deberá ser aprobado para la ejecución del mismo.

b. Cada jefe de área y persona con activo asignado, deberá proporcionar toda información sobre los activos a su cargo desde el inicio y de los que se les ha sido entregado durante el periodo de desempeño de sus funciones.

c. Los formularios del control de inventario serán contrastados con los registros actuales.

d. En caso de existir diferencia de información, se deberá presentar los respaldos de las asignaciones de inventario, los mismos que deberán registrar las firmas del empleado.

4.6 ACTIVO: A06 ARCHIVO VIDA LABORAL DE EMPLEADOS

4.6.1 Amenaza: Divulgación de la información

Control 8.1.3 Términos y condiciones del empleo
Recomendación
La empresa debe establecer un acuerdo de confidencialidad al momento de firmar el contrato laboral; en el mismo se debe manifestar la ***no divulgación*** de toda información personal en lo que a empleados se refiere y a la de único interés y de uso exclusivo del Organismo.

Política de seguridad

-Todo empleado que inicie su relación laboral con el Organismo, firmará un documento llamado de ***confidencialidad*** que será entregado por RRHH en el momento de la contratación, el mismo que está obligado a cumplir en un periodo de 3 meses después de concluida dicha relación.

Procedimiento

a. El Departamento legal, en conjunto con RRHH y la Dirección del Hospital redactarán un documento de ***confidencialidad***; en el que se obliga al empleado a la no divulgación, ni exposición de toda información que incluya datos de uso exclusivo del Organismo.
b. Este documento deberá ser firmado por cada uno de los empleados en el momento de la contratación.
c. El documento de confidencialidad tendrá vigencia de 3 meses adicionales una vez concluida la relación laboral Empleado-Organismo.

Control 8.3.1 Responsabilidades de terminación
Política de Seguridad

- Una vez que el ex empleado cese sus funciones dentro de la Organización, está obligado a cumplir con la no divulgación de la información de uso exclusivo del Organismo

Procedimiento
Cuando un empleado cese sus funciones o el empleado cambie de funciones dentro de la organización, está obligado a cumplir con el acuerdo de confidencialidad; es decir a la no divulgación de la información durante un periodo de 3 meses finalizado el contrato.

Control 8.3.3 Retiro de los derechos de acceso
Política de Seguridad

-Cuando un empleado cambia su situación laboral, el acceso que este tiene a la información será inhabilitado 24 horas antes de la entrega del documento de acción de personal en el que se comunica el cese o cambio de sus funciones dentro del Organismo; y 24 horas después en caso de renuncia voluntaria sin previo aviso.

-Los derechos de acceso que deberían ser retirados o adaptados incluyen accesos físicos y lógicos, claves, tarjetas de identificación, recursos de tratamiento de la información, suscripciones, así como la retirada de cualquier documentación que les identifique como un miembro actual de la organización.

Procedimiento

a. En caso de renuncia voluntaria, despido forzado, del área de RRHH emitirá la ***acción de personal*** (anexo II), en el que se especifica los motivos por el cual el empleado es despedido o procede al cambio de sus funciones.
b. Si el empleado que procede a la modificación de su relación laboral, pertenece a alguna de las áreas administrativas en las que se tiene acceso a la información digital, se enviará una copia del documento al Centro de Cómputo para la verificación y posterior inhabilitación de los accesos en caso de los que tuviere del empleado.
c. En caso de cambio de sus funciones, un asistente del centro de cómputo y el jefe de la próxima área del empleado, plantearán las modificaciones de los accesos que necesitará para el desarrollo de las obligaciones establecidas.

4.6.2 Amenaza: Interceptación de la Información

Control 8.3.3 Retiro de los derechos de acceso
Política de Seguridad

-Cuando un empleado cambia su situación laboral, el acceso que este tiene a la información será inhabilitado 24 horas antes de la entrega del documento de acción de personal en el que se comunica el cese o cambio de sus funciones dentro del Organismo; y 24 horas después en caso de renuncia voluntaria sin previo aviso.

-Los derechos de acceso que deberían ser retirados o adaptados incluyen accesos físicos y lógicos, claves, tarjetas de identificación, recursos de tratamiento de la información, suscripciones, así como la retirada de cualquier documentación que les identifique como un miembro actual de la organización.

Procedimiento

a. En caso de renuncia voluntaria, despido forzado, del área de RRHH emitirá la ***acción de personal*** (anexo II), en el que se especifica los motivos por el cual el empleado es despedido o procede al cambio de sus funciones.
b. Si el empleado pertenece a alguna de las áreas administrativas en las que se tiene acceso a la información digital, se enviará una copia del documento al Centro de Cómputo para la verificación y posterior inhabilitación de los accesos en caso de los que tuviere del empleado.
c. Si el empleado pertenece a alguna de las áreas administrativas en las que se tiene acceso a las áreas restringidas, el jefe inmediato comunicará la retirada de la tarjeta de acceso o la anulación del registro dactilar dependiendo de la infraestructura instalada.
d. En caso de cambio de sus funciones, un asistente del centro de cómputo y el jefe de la próxima área del empleado, plantearán las modificaciones de los accesos que necesitará para el desarrollo de las obligaciones establecidas.

4.7 ACTIVO: A07 ARCHIVO DE PACIENTES

4.7.1 Amenaza: Divulgación de la Información

Control 8.1.3 Términos y condiciones del empleo
Recomendación
La empresa debe establecer un acuerdo de confidencialidad al momento de firmar el contrato laboral; en el mismo se debe manifestar la ***no divulgación*** de toda información personal en lo que a empleados se refiere y a la de único interés y de uso exclusivo del Organismo.

Política de seguridad

-Todo empleado que inicie su relación laboral con el Organismo, firmará un documento llamado de ***confidencialidad*** que será entregado por RRHH en el momento de la contratación, el mismo que está obligado a cumplir en un periodo de 3 meses después de concluida dicha relación.

Procedimiento

a. El Departamento legal, en conjunto con RRHH y la Dirección del Hospital redactarán un documento de ***confidencialidad***; en el que se obliga al empleado a la no divulgación, ni exposición de toda información que incluya datos de uso exclusivo del Organismo.
b. Este documento deberá ser firmado por cada uno de los empleados en el momento de la contratación.
c. El documento de confidencialidad tendrá vigencia de 3 meses adicionales una vez concluida la relación laboral Empleado-Organismo.

Control 8.3.1 Responsabilidades de terminación
Política de Seguridad

- Una vez que el ex empleado cese sus funciones dentro de la Organización, está obligado a cumplir con la no divulgación de la información de uso exclusivo del Organismo

Procedimiento

a.Una vez que el ex empleado cese sus funciones o el empleado cambie de funciones dentro de la organización, está obligado a cumplir con el acuerdo de confidencialidad; es decir a la no divulgación de la información durante un periodo de 3 meses finalizado el contrato.

4.7.2 Amenaza: Manipulación de la Información

Control 8.3.2 Devolución de los activos
Política de Seguridad

- Todos los activos de las diferentes áreas deberán ser devueltos en perfecto estado, ya sean estas a nivel médico o administrativo.
- Si existe algún activo que no pertenezca al Organismo este será revisado para verificar si tiene información relevante para la organización, si es así, esta será entregada al Organismo.

Procedimiento

a. Los empleados deberán llenar un formulario de devolución de activos entregado por el departamento de inventario en el cual indicaran todos los activos que el Organismo les entrego; a su vez indicaran los activos propios del empleado, que utilizó en el Organismo durante su función.
b. Una vez declarados los activos estos serán entregados y revisados para ver su buen estado, si el activo tiene algún daño se evaluará su reparación o reposición del mismo.
c. Si el activo del empleado contiene información relevante para el Organismo esta deberá ser entregada y eliminada del activo del empleado.
d. Si todos los procesos anteriores se llevaron a cabo el empleado firmará el formulario de devolución de activos dejando constancia de dicho proceso.

Control 8.3.3 Retiro de los derechos de acceso
Política de Seguridad

-Cuando un empleado cambia su situación laboral, el acceso que este tiene a la información será inhabilitado 24 horas antes de la entrega del documento de acción de personal en el que se comunica el cese o cambio de sus funciones dentro del Organismo; y 24 horas después en caso de renuncia voluntaria sin previo aviso.

-Los derechos de acceso que deberían ser retirados o adaptados incluyen accesos físicos y lógicos, claves, tarjetas de identificación, recursos de tratamiento de la información, suscripciones, así como la retirada de cualquier documentación que les identifique como un miembro actual de la organización.

Procedimiento

a. En caso de renuncia voluntaria, despido forzado, del área de RRHH emitirá la ***acción de personal*** (anexo II), en el que se especifica los motivos por el cual el empleado es despedido o procede al cambio de sus funciones.
b. Si el empleado pertenece a alguna de las áreas administrativas en las que se tiene acceso a la información digital, se enviará una copia del documento al Centro de
c. Cómputo para la verificación y posterior inhabilitación de los accesos en caso de los que tuviere del empleado.
d. Si el empleado pertenece a alguna de las áreas administrativas en las que se tiene acceso a las áreas restringidas, el jefe inmediato comunicará la retirada de la tarjeta de acceso o la anulación del registro dactilar dependiendo de la infraestructura instalada.
e. En caso de cambio de sus funciones, un asistente del centro de cómputo y el jefe de la próxima área del empleado, plantearán las modificaciones de los accesos que necesitará para el desarrollo de las obligaciones establecidas.

4.7.3 Amenaza: Acceso no Autorizado

Control: 9.1.3 Seguridad de oficinas, despachos e instalaciones
Recomendación
Se recomienda que en el departamento de Estadística seguridades tales como puertas de acceso controladas con tarjetas o con identificadores de huellas dactilares; de esta forma poder proteger aquella área donde se archivan cada una de las carpetas con las historias clínicas de los pacientes.
Además se debería controlar la retirada de las carpetas con las historias clínicas con un periodo máximo, así de esta manera se obligará la devolución de la misma cuando expire su tiempo, comunicando al médico a cargo su devolución.

Política de Seguridad
-El acceso a áreas restringidas será controlado mediante puertas con apertura de lector dactilar.
-El área de Estadística será considerado como área de acceso restringido.
-El área de archivo de RRHH será considerado como área de acceso restringido

Control 8.3.3 Retiro de los derechos de acceso
Política de Seguridad

-Cuando un empleado cambia su situación laboral, el acceso que este tiene a la información será inhabilitado 24 horas antes de la entrega del documento de en el que se comunica el cese o cambio de sus funciones dentro del Organismo; y 24 horas después en caso de renuncia voluntaria sin previo aviso.

-Los derechos de acceso que deberían ser retirados o adaptados incluyen accesos físicos y lógicos, claves, tarjetas de identificación, recursos de tratamiento de la información, suscripciones, así como la retirada de cualquier documentación que les identifique como un miembro actual de la organización.

Procedimiento

a. En caso de renuncia voluntaria, despido forzado, del área de RRHH emitirá la ***acción de personal*** (anexo II), en el que se especifica los motivos por el cual el empleado es despedido o procede al cambio de sus funciones.
b. Si el empleado pertenece a alguna de las áreas administrativas en las que se tiene acceso a la información digital, se enviará una copia del documento al Centro de Cómputo para la verificación y posterior inhabilitación de los accesos en caso de los que tuviere del empleado.
c. Si el empleado pertenece a alguna de las áreas administrativas en las que se tiene acceso a las áreas restringidas, el jefe inmediato comunicará la retirada de la tarjeta de acceso o la anulación del registro dactilar dependiendo de la infraestructura instalada.
d. En caso de cambio de sus funciones, un asistente del centro de cómputo y el jefe de la próxima área del empleado, plantearán las modificaciones de los accesos que necesitará para el desarrollo de las obligaciones establecidas.

4.7.4 Amenaza: Interceptación de la Información

Control 8.1.3 Términos y condiciones del empleo
Recomendación
La empresa debe establecer un acuerdo de confidencialidad al momento de firmar el contrato laboral; en el mismo se debe manifestar la ***no divulgación*** de toda información personal en lo que a empleados se refiere y a la de único interés y de uso exclusivo del Organismo.

Política de seguridad

-Todo empleado que inicie su relación laboral con el Organismo, firmará un documento llamado de ***confidencialidad*** que será entregado por RRHH en el momento de la contratación, el mismo que está obligado a cumplir en un periodo de 3 meses después de concluida dicha relación.

Procedimiento

a. El Departamento legal, en conjunto con RRHH y la Dirección del Hospital redactarán un documento de ***confidencialidad***; en el que se obliga al empleado a la no divulgación, ni exposición de toda información que incluya datos de uso exclusivo del Organismo.
b. Este documento deberá ser firmado por cada uno de los empleados en el momento de la contratación.
c. El documento de confidencialidad tendrá vigencia de 3 meses adicionales una vez concluida la relación laboral Empleado-Organismo.

Control 8.3.1 Responsabilidades de terminación
Política de Seguridad

- Una vez que el ex empleado cese sus funciones dentro de la Organización, está obligado a cumplir con la no divulgación de la información de uso exclusivo del Organismo**.**

Procedimiento
Cuando un empleado cese sus funciones o el empleado cambie de funciones dentro de la organización, está obligado a cumplir con el acuerdo de confidencialidad; es decir a la no divulgación de la información durante un periodo de 3 meses finalizado el contrato.

Control 8.3.3 Retiro de los derechos de acceso
Política de Seguridad

-Cuando un empleado cambia su situación laboral, el acceso que este tiene a la información será inhabilitado 24 horas antes de la entrega del documento de acción de personal en el que se comunica el cese o cambio de sus funciones dentro del Organismo; y 24 horas después en caso de renuncia voluntaria sin previo aviso.

-Los derechos de acceso que deberían ser retirados o adaptados incluyen accesos físicos y lógicos, claves, tarjetas de identificación, recursos de tratamiento de la

información, suscripciones, así como la retirada de cualquier documentación que les identifique como un miembro actual de la organización.

Procedimiento

a. En caso de renuncia voluntaria, despido forzado, del área de RRHH emitirá la ***acción de personal*** (anexo II), en el que se especifica los motivos por el cual el empleado es despedido o procede al cambio de sus funciones.
b. Si el empleado pertenece a alguna de las áreas administrativas en las que se tiene acceso a la información digital, se enviará una copia del documento al Centro de Cómputo para la verificación y posterior inhabilitación de los accesos en caso de los que tuviere del empleado.
c. Si el empleado pertenece a alguna de las áreas administrativas en las que se tiene acceso a las áreas restringidas, el jefe inmediato comunicará la retirada de la tarjeta de acceso o la anulación del registro dactilar dependiendo de la infraestructura instalada.
d. En caso de cambio de sus funciones, un asistente del centro de cómputo y el jefe de la próxima área del empleado, plantearán las modificaciones de los accesos que necesitará para el desarrollo de las obligaciones establecidas.

4.7.5 Amenaza: Corrupción de la Información

Control 8.3.2 Devolución de los activos

Política de Seguridad

-Todos los activos de las diferentes áreas deberán ser devueltos en perfecto estado, ya sean estas a nivel médico o administrativo.
-Si existe algún activo que no pertenezca al Organismo este será revisado para verificar si tiene información relevante para la organización, si es así, esta será entregada al Organismo.

Procedimiento

a. Los empleados deberán llenar un formulario de devolución de activos entregado por el departamento de inventario en el cual indicaran todos los activos que el Organismo les entrego; a su vez indicaran los activos propios del empleado, que utilizó en el Organismo durante su función.
b. Una vez declarados los activos estos serán entregados y revisados para ver su buen estado, si el activo tiene algún daño se evaluará su reparación o reposición del mismo.
c. Si el activo del empleado contiene información relevante para el Organismo esta deberá ser entregada y eliminada del activo del empleado.
d. Si todos los procesos anteriores se llevaron a cabo el empleado firmará el formulario de devolución de activos dejando constancia de dicho proceso.

Control 8.3.3 Retiro de los derechos de acceso

Política de Seguridad

-Cuando un empleado cambia su situación laboral, el acceso que este tiene a la información será inhabilitado 24 horas antes de la entrega del documento de acción de personal en el que se comunica el cese o cambio de sus funciones

dentro del Organismo; y 24 horas después en caso de renuncia voluntaria sin previo aviso.

-Los derechos de acceso que deberían ser retirados o adaptados incluyen accesos físicos y lógicos, claves, tarjetas de identificación, recursos de tratamiento de la información, suscripciones, así como la retirada de cualquier documentación que les identifique como un miembro actual de la organización.

Procedimiento

a. En caso de renuncia voluntaria, despido forzado, del área de RRHH emitirá la ***acción de personal*** (anexo II), en el que se especifica los motivos por el cual el empleado es despedido o procede al cambio de sus funciones.
b. Si el empleado pertenece a alguna de las áreas administrativas en las que se tiene acceso a la información digital, se enviará una copia del documento al Centro de Cómputo para la verificación y posterior inhabilitación de los accesos en caso de los que tuviere del empleado.
c. Si el empleado pertenece a alguna de las áreas administrativas en las que se tiene acceso a las áreas restringidas, el jefe inmediato comunicará la retirada de la tarjeta de acceso o la anulación del registro dactilar dependiendo de la infraestructura instalada.
d. En caso de cambio de sus funciones, un asistente del centro de cómputo y el jefe de la próxima área del empleado, plantearán las modificaciones de los accesos que necesitará para el desarrollo de las obligaciones establecidas.

4.8 ACTIVO: S01 PC

4.8.1 Amenaza: Uso indebido

Existen muchas razones para establecer un control estricto en lo que a redes sociales se refiere, entre otro tenemos:

•Fuga de datos: usualmente los usuarios de las redes sociales comparten más información de la necesaria ya sea de manera voluntaria o involuntaria.

•Robo de información: las redes de sociales contienen gran cantidad de información que está disponible libremente para millones de personas.

•Implicaciones legales: es necesario estar al tanto de las implicaciones que puede tener para su compañía la información publicada por sus empleados en las redes sociales.

•Malware: diversas aplicaciones de las redes sociales son punto de entrada de diferentes tipos de malware (en especial para robar información confidencial).

•Ingeniería Social: los usuarios de las redes sociales son altamente propensos a ataques de ingeniería social. En especial empleados clave.

Política de Seguridad

-Queda prohibido el acceso a redes sociales, redes comerciales, en general al acceso a direcciones electrónicas y sitios que se consideran innecesarios para cuestiones laborales de cada uno de los puestos del organismo.

Procedimiento
El centro de cómputo será el encargado de implementar las medidas necesarias para la puesta en marcha de esta política de seguridad.

4.9 ACTIVO: D01 DIRECTOR GENERAL

4.9.1Amenaza: Deficiencia en la organización

Cada vez más necesario que las empresas implanten programas de adiestramiento que a través de estos les permita a sus empleados satisfacer sus objetivos personales, laborales y de esta manera el organismo cuente con un personal altamente calificado, a través del aumento de la productividad, la planificación de carrera y la calidad de vida de los empleados.

Control 8.1.1 Roles y responsabilidades
Política de seguridad
-Se establece la obligación de documentar las responsabilidades y funciones de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización, estableciendo por escrito, de alguna forma las obligaciones del puesto con el Organismo.

Procedimiento

a. El departamento de RRHH será el encargado de realizar un manual de funciones y servicios, donde se especifique por escrito el desempeño del puesto a cubrir, pudiendo así el organismo en el momento del cese laboral, reclamar y ejercer el derecho de cumplimiento de dichas funciones y la fiscalización de lo ejercido por el empleado.
b. El empleado recibirá la documentación de cada una de sus funciones al inicio de su relación laboral, dejando constancia de recibido.

4.10 ACTIVO: D02 JEFES DE ÁREA

4.10.1Amenaza: Deficiencia de la organización

Que las empresas implanten programas de adiestramiento sería una buena inversión ya que a través de estos les permite a sus empleados satisfacer sus objetivos personales, laborales; el organismo podrá contar así con un personal altamente calificado.

Control 8.1.1 Roles y responsabilidades
Política de seguridad
-Se establece la obligación de documentar las responsabilidades y funciones de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización, estableciendo por escrito, de alguna forma, las obligaciones del empleado con el puesto y con el Organismo.

Procedimiento

a. El departamento de RRHH será el encargado de realizar un manual de funciones y servicios, donde se especifique por escrito el desempeño del puesto a cubrir, pudiendo así el organismo en el momento del cese laboral, reclamar y ejercer el derecho del cumplimiento de dichas funciones y la fiscalización de lo ejercido por el empleado.
b. El empleado recibirá la documentación de cada una de sus funciones al inicio de su relación laboral, dejando constancia de recibido.

4.11 ACTIVO: H01 ÁREAS RESTRINGIDAS

4.11.1 Amenaza: Uso no previsto

Control: 9.1.2 Controles de acceso físico

Recomendación

Se implementará en las áreas restringidas, la adecuada protección del acceso físico del personal; para asegurar así solamente el acceso autorizado.

Política de Seguridad

-El acceso a áreas restringidas será controlado mediante puertas con apertura de lector dactilar o con tarjetas de acceso.

4.11.2 Amenaza: Acceso no autorizado

Control: 9.1.2 Controles de acceso físico

Recomendación

Se implementará en las áreas restringidas, la adecuada protección del acceso físico del personal; para asegurar así solamente el acceso autorizado.

Política de Seguridad

-El acceso a áreas restringidas será controlado mediante puertas con apertura de lector dactilar o con tarjetas de acceso

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5 CONCLUSIONES Y RECOMENDACIONES

En el desarrollo del presente capítulo se exponen las conclusiones y las recomendaciones de la tesis de grado, realizados sobre la base de los objetivos que tiene el presente trabajo, tales como: Realizar los debidos procedimientos desde la contratación hasta el despido o cese de funciones del empleado.

Entre las conclusiones que pudimos observar se encuentran las siguientes:

- El hospital cuenta con una aplicación que está conectado con el IESS (Instituto Ecuatoriano de Seguridad Social) y el Ministerio de Finanzas el cual posee algunas fallas entre las cuales está que las ventanas de la aplicación muchas veces se bloquean o son imposibles de acceder.

- Existe otra aplicación la cual permite el control de asistencia de los empleados. Está en proyecto la conexión directa de esta aplicación con el Ministerio de Relaciones Laborales.

- Trabajan bajo las normativas de la LOSEP (Ley Orgánica del Servicio Público). Cada movimiento, proceso o toma de decisión se basa en la LOSEP

- Los trabajadores se dividen en dos grupos: Los amparados bajos la LOSEP como (médicos, enfermeras) y los trabajadores amparados por el código del trabajo tales como: (choferes, electricistas, cocineros).

- Entre los procesos de movimiento del personal están los siguientes:
  1.- Reclutamiento o selección.
  2.- Clasificación de puestos.
  3.- Sistema de evaluación o desempeño
  4.- Capacitación.
  5.- Planificación
  6.- Evaluación de desempeño.

1.- Reclutamiento o selección.

Existen dos vías:

a.- norma técnica de selección y concursos
b.- instructivo para llenar vacantes

1.1 Orden

El Director (Responsable directo) llama a concurso.
El Jefe de recursos humanos es notificado por el Director y llama a concurso y Determina las personas responsable para la selección del personal.

1.2 Tribunal

Dependiendo lo que ordene el reglamento los concursos serán abiertos (pueden acceder cualquier ciudadano que cumpla los requisitos; o cerrados (solo personal del hospital).
El tribunal está conformado por: El Responsable de dirección del hospital, responsable de RRHH, responsable del organismo sindical y el responsable del área de necesidad. Las calificaciones dependen de un examen teórico y de la entrevista personal.

2.- Clasificación o actualización del personal.

Analistas de Quito 1 vez al año actualizan cada uno de los puestos cubiertos en el hospital, ya sea por que el empleado ha recibido mayor formación o por que este a nivel de experiencia pueda desenvolver un puesto con mayor responsabilidad, de esta forma pueda ascender a otro nivel y aumentar así su remuneración mensual.Para esto los analistas se basan en una tabla de clasificación de puestos y además cada acción será acatada bajo alguna norma técnica.

3.- Evaluación por desempeño.

Existen grados de evaluación para cada personal; estos van desde (excelente, hasta malo), esto sirve para poder realizar movimientos en el personal ya sea por (baja, ascenso, capacitación, etc.).Estas evaluaciones están a cargo del jefe de RRHH y del jefe inmediato del área al que pertenece el empleado.

4.-Capacitación

Las capacitaciones son programadas anualmente; al ser dependientes del estado poco es el presupuesto destinado a los mismos, por eso se solventan en base de las multas establecidas para cada sanción del personal, en las aportaciones del Ministerio, y en los diferentes acuerdos entre las empresas capacitadoras que colaboran con el hospital.

5.- Planificación

Esta norma tiene como finalidad la creación de puestos y la anulación de los mismos. Las bajas o despidos están clasificadas en:

Renuncias.
Muerte.
Jubilación obligada (mayores de 65 años).
Jubilación voluntaria.
Destitución por sumario administrativo.
Destitución por sanción.
Supresión de puestos mediante acción de personal y posterior bonificación.

- El departamento está bajo auditorías periódicas y cada movimiento o modificación se realiza bajo la firma del jefe de personal.

Entre las recomendaciones que pudimos observar se encuentran las siguientes:

- La empresa debe establecer un acuerdo de confidencialidad al momento de firmar el contrato laboral; en el mismo se debe manifestar la no divulgación de toda información personal en lo que a empleados se refiere y a la de único interés y de uso exclusivo del Organismo.

- Se recomienda que en el archivo de RRHH se instalen seguridades tales como puertas de acceso controladas con tarjetas o con identificadores de huellas dactilares; de esta forma poder proteger aquella área donde se archivan cada una de las carpetas con la vida laboral de cada uno de los empleados.

- Se recomienda que en el departamento de Estadística seguridades tales como puertas de acceso controladas con tarjetas o con identificadores de huellas dactilares; de esta forma poder proteger aquella área donde se archivan cada una de las carpetas con las historias clínicas de los pacientes.

  Además se debería controlar la retirada de las carpetas con las historias clínicas con un periodo máximo, así de esta manera se obligará la devolución de la misma cuando expire su tiempo, comunicando al médico a cargo su devolución.

- Se implementará en las áreas restringidas, la adecuada protección del acceso físico del personal; para asegurar así solamente el acceso autorizado.

CAPÍTULO 6

ANEXOS

6 ANEXOS

6.1 ANEXO I

6.1.1 Hoja de Inventario

DIRECCION PROVINCIAL DE SALUD DEL GUAYAS
HOSPITAL DEL NIÑO "DR. FRANCISCO DE ICAZA BUSTAMANTE"
DIRECCION DE GESTION ADMINISTRATIVA
UNIDAD DE ACTIVO FIJOS
INVENTARIO PARCIAL Y CONSTATACION FISICA DE LOS ACTIVOS FIJOS
BIENES DE LARGA DURACION

PROCESO			
SUBPROCESO		ANESTESIOLOGIA	

En la ciudad de Guayaquil a los 30 días del mes de NOVIEMBRE del 2010, de conformidad con los articulos 2, 3, 90 y 92 del Reglamento General Sustitutivos para el Manejo y Administración de bienes del Sector Publico y los articulos 11 y 26 del Reglamento Interno para el Control de Activos Fijos del MSP, se procede a la constatación física de los bienes que se detallan a continuación y que se encuentra bajo custodia de la Dra. SARA VELASQUEZ JARA, servidora del Ministerio de Salud Publica, Hospital del Niño "Dr. Francisco de Icaza Bustamante; para constancia los involucrados suscriben el presente formulario:

		DESCRIPCION								
CANTIDAD	CODIGO	NOMBRE DEL BIEN	FECHA ING	Nº INGRESO	MARCA	SERIE	MODELO	ESTADO	V.UNIT.	V. TOTAL

6.2 ANEXO II

6.2.1 Dominios del Sistema de Gestión de Seguridad de la Información:

Cada uno de los dominios conforma un capítulo de la norma y se centra en un determinado aspecto de la seguridad de la información. En el siguiente dibujo se muestra la distribución de dichos dominios y el aspecto de seguridad que cubren:

Distribución de los dominios de la Norma ISO 27002

6.3 ANEXO III

6.3.1ACCIÓN DE PERSONAL

REPUBLICA DEL ECUADOR	**ACCION DE PERSONAL**	Ministerio de Salud Pública
HOSPITAL PEDIÁTRICO "Dr. Francisco de Ycaza Bustamante"	3) ☐ Decreto ☒ Acuerdo ☐ Resolución No.: 112 Fecha: 1 DE ABRIL DEL 2011	4) No.: 1254 - HN-UATH-2011 FECHA: 1 DE ABRIL DEL 2011
5) **SR. CABERO AYORA RICHARD FABIAN** APELLIDOS NOMBRES		2)Cédula de Ciudadanía No.: 1206753103

6a) No. Afiliación al IESS	6b) No. Libreta Militar	6c) Comprobante de Votación No.:	6d) RIGE A PARTIR: 31 DE MARZO DEL 2011

7)	8) EXPLICACIÓN
☐ Nombramiento Regular ☐ Nombramiento Provisional ☐ Ascenso o Traslado ☐ Vacaciones ☐ Licencia o Permiso ☐ Renuncia ☐ Sanción disciplinaria ☐ Destitución ☐ Supresión de partida ☒ Otros (AGRADECIMIENTO)	**ACUERDA** CESAR EN SUS FUNCIONES POR HABER FINALIZADO SU PERIODO FIJO DE NOMBRAMIENTO PROVISIONAL AL SR. CABERO AYORA RICHARD FABIAN, OCUPANTE DEL PUESTO QUE SE EXPLICA EN LA CASILLA NO.9 Y AGRADECERLE POR LOS SERVICIOS PRESTADOS A LA INSTITUCION. DE CONFORMIDAD CON LO ESTABLECIDO EN EL ART.47 Literal e) DE LA LEY ORGANICA DEL SERVICIO PUBLICO.

9) **SITUACIÓN INICIAL**	10) **SITUACIÓN PROPUESTA**
DIRECCIÓN PROVINCIAL DE SALUD DEL GUAYAS HOSPITAL PEDIÁTRICO "DR. "FRANCISCO DE YCAZA BUSTAMANTE" PROCESO: GOBERNANTE GESTION: DIRECCION PUESTO: SERVIDOR PUBLICO DE APOYO 1-ASISTENTE ADMINISTRATIVO LUGAR DE TRABAJO: **GUAYAQUIL** SUELDO UNIFICADO USD: USD 555.00 PARTIDA PRESUPUESTARIA No.20113201190000020000000 03G9151010509010010000000-15	DIRECCIÓN PROVINCIAL DE SALUD DEL GUAYAS HOSPITAL PEDIATRICO "DR. "FRANCISCO DE YCAZA BUSTAMANTE" PROCESO: SUBPROCESO: GESTION: PUESTO: LUGAR DE TRABAJO: SUELDO UNIFICADO: PARTIDA PRESUPUESTARIA No.
(Vto. Bno.) Oficio No. Fecha:	11) **OFICINA DE RECURSOS HUMANOS** Participo en Concurso No.: Fecha: Abg. Jesús García Cedeño **f) COORDINADOR DE LA UATH**

2) Y por el Ministerio de Salud Pública, autorizado mediante Acuerdo Ministerial No.1726 del 13 de octubre de 1999 (Registro Oficial No.310 del 3 de noviembre de 1999)

Dr. Javier Chacón Cantos
Marisela Alvarado **GERENTE DE HOSPITAL**

DEPARTAMENTO DE RECUR SOS HUMANOS

REVISADO

Registro No.: Fecha: ANALISTA RESPONSABLE

6.4 ANEXO IV

6.4.1 POLÍTICAS DE SEGURIDAD

Las siguientes políticas de seguridad deberán ser implantadas para disminuir el nivel de riesgo que generan las amenazas encontradas. La aplicación de las mismas son necesarias para la certificación de la ISO 27001.

Art 01

- Se documentará las responsabilidades y funciones de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización, estableciendo por escrito, de alguna forma, las obligaciones del empleado con el puesto y con el Organismo.

Art 02

- Todo empleado que inicie su relación laboral con el Organismo, firmará un documento llamado de ***confidencialidad*** que será entregado por RRHH en el momento de la contratación, el mismo que está obligado a cumplir en un periodo de 3 meses después de concluida dicha relación.

Art 03

- Una vez que el ex empleado cese sus funciones dentro de la Organización, está obligado a cumplir con la no divulgación de la información de uso exclusivo del Organismo

Art 04

- Todos los activos de las diferentes áreas deberán ser devueltos en perfecto estado, ya sean estas a nivel médico o administrativo.

- Si existe algún activo que no pertenezca al Organismo este será revisado para verificar si tiene información relevante para la organización, si es así, esta será entregada al Organismo.

Art 05

- Cuando un empleado cambia su situación laboral, el acceso que este tiene a la información será inhabilitado 24 horas antes de la entrega del documento de acción de personal en el que se comunica el cese o cambio de sus funciones dentro del Organismo; y 24 horas después en caso de renuncia voluntaria sin previo aviso.

- Los derechos de acceso que deberían ser retirados o adaptados incluyen accesos físicos y lógicos, claves, tarjetas de identificación, recursos de tratamiento de la información, suscripciones, así como la retirada de cualquier documentación que les identifique como un miembro actual de la organización.

Art 06

- El acceso a áreas restringidas será controlado mediante puertas con apertura de lector dactilar o con tarjetas de acceso.

- El área de Estadística será considerado como área de acceso restringido.

- El área de archivo de RRHH será considerado como área de acceso restringido

Art 07

- Queda prohibido el acceso a redes sociales, redes comerciales, en general al acceso a direcciones electrónicas y sitios que se consideran innecesarios para cuestiones laborales de cada uno de los puestos del organismo.

Art 08

- El control de inventario de activos se realizará cada tres meses, en el cual cada empleado deberá confirmar los activos asignados al inicio de sus funciones

Art 09

- El control de inventario de activos se realizará cada tres meses, en el cual cada empleado deberá confirmar los activos asignados al inicio de sus funciones.

6.5 ANEXO V

6.5.1 Marco de referencia

6.5.1.1 ¿Qué es seguridad de la información?

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización y que podría considerarse como el sistema de calidad para la seguridad de la información.

Prometer o garantizar un nivel de protección al 100% en todas las áreas es virtualmente imposible, incluso en el caso de que podamos disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a cualquier cambio que se produzca, ya sean estos en los riesgos, el entorno y las tecnologías.

6.5.2 ¿Qué es un SGSI?

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

Un SGSI es un Sistema que consiste de una serie de actividades de gestión que deben realizarse mediante procesos sistemáticos, documentados y conocidos por una organización o entidad.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

El propósito de un sistema de gestión de la seguridad de la información no es garantizar la seguridad – que nunca podrá ser absoluta- sino garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías.

El SGSI protege los activos de información de una organización, independientemente del medio en que se encuentren; p. ej., correos electrónicos, informes, escritos relevantes, páginas web, imágenes, documentos, hojas de cálculo, faxes, presentaciones,

contratos, registros de clientes, información confidencial de trabajadores y colaboradores, entre otros.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad, disponibilidad y legalidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos cuatro términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

Fig. F.12 SGSI Principios básicos.

- ***Integridad***: Mantener la exactitud y completitud de la información y sus métodos de proceso.

- ***Privacidad***: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- ***Disponibilidad***: El acceso y la utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- ***Legalidad***: La información debe de cumplir con las leyes vigentes dependiendo del lugar donde se encuentran y son manejadas.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

6.5.3 ¿Para qué sirve un SGSI?

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y por consecuente su información, están expuestos cada vez más a un número elevado de amenazas que aprovechan cualquiera de las vulnerabilidades existentes para someter a activos críticos de información, a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados desde dentro de la propia organización ya sean estos voluntaria o involuntariamente, o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos los cuales son difíciles de prevenir y de manejar.

Cumplir con las leyes establecidas, poder adaptarse de forma dinámica y puntual a las condiciones variables del entorno, proteger adecuadamente los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios.

El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

6.5.4 ISO (International Organization for Standardization)

La ISO es una federación internacional con sede en Ginebra (Suiza) de los institutos de normalización de 157 países (uno por cada país). Es una organización no gubernamental (sus miembros no son delegados de gobiernos nacionales), puesto que el origen de los institutos de normalización nacionales es diferente en cada país (entidad pública, privada).

La ISO desarrolla estándares requeridos por el mercado que representan un consenso de sus miembros (previo consenso nacional entre industrias, expertos, gobierno, usuarios, consumidores) acerca de productos, tecnologías, sistemas y métodos de gestión, entre otros.
Estos estándares, por naturaleza, son de aplicación voluntaria, ya que el carácter no gubernamental de ISO no le da autoridad legal para forzar su implantación. Sólo en aquellos casos en los que un país ha decidido adoptar un determinado estándar como parte de su legislación, puede convertirse en obligatorio.

La ISO garantiza un marco de amplia aceptación mundial a través de sus 3.000 grupos técnicos y más de 50.000 expertos que colaboran en el desarrollo de estándares.

6.5.4.1 ISO 27000

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001.

6.5.4.1.1 *Origen*

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

1979 Publicación BS 5750 - ahora ISO 9001

1992 Publicación BS 7750 - ahora ISO 14001

1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.
En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

En la sección de Artículos y Podcasts encontrará un archivo gráfico y sonoro con la historia de ISO 27001 e ISO 17799.

6.5.4.1.2 *La serie 27000*

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

• ISO 27000:
En fase de desarrollo; su fecha prevista de publicación es Noviembre de 2008. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma está previsto que sea gratuita, a diferencia de las demás de la serie, que tendrán un coste.

• 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. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones.

Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007 y puede adquirirse online en AENOR.

Otros países donde también está publicada en español son, por ejemplo, Colombia, Venezuela y Argentina. El original en inglés y la traducción al francés pueden adquirirse en ISO.org.

• 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. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005. En España, aún no está traducida (previsiblemente, a lo largo de 2008). Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en ISO.org.

• ISO 27003:
En fase de desarrollo; su fecha prevista de publicación es Mayo de 2009. Consistirá en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

• ISO 27004:
En fase de desarrollo; su fecha prevista de publicación es Noviembre de 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.

• 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. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de

lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 y ISO/IEC TR 13335-4:2000.

En España, esta norma aún no está traducida. El original en inglés puede adquirirse en ISO.org.

• ISO 27006:
Publicada el 13 de Febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSI) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específico relacionados con ISO 27001 y los SGSI. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. En España, esta norma aún no está traducida. El original en inglés puede adquirirse en ISO.org.

• ISO 27007:
En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de auditoría de un SGSI.

• ISO 27011:
En fase de desarrollo; su fecha prevista de publicación es Enero de 2008. Consistirá en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

• ISO 27031:
En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

• ISO 27032:
En fase de desarrollo; su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía relativa a la ciberseguridad.

• ISO 27033:
En fase de desarrollo; su fecha prevista de publicación es entre 2010 y 2011. Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y re-numeración de ISO 18028.

• ISO 27034:
En fase de desarrollo; su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía de seguridad en aplicaciones.

• ISO 27799:
Publicada el 12 de Junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma. ISO 27799:2008 especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud. ISO 27799:2008 se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas, toma la información (palabras y números, grabaciones sonoras, dibujos, vídeos e imágenes médicas), sea cual fuere el medio utilizado para almacenar (de impresión o de escritura en papel o electrónicos de almacenamiento) y sea cual fuere el medio utilizado para transmitirlo (a mano, por fax, por redes informáticas o por correo), ya que la información siempre debe estar adecuadamente protegida. El original en inglés o francés puede adquirirse en ISO.org.

6.5.5 Metodología ISO27001

Es un estándar ISO que proporciona un modelo para establecer, implementar, utilizar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en el ciclo de vida PDCA (Planear-Hacer-Verificar-Actuar; o ciclo de Deming) de mejora continua, al igual que otras normas de sistemas de gestión (ISO 9001 para calidad, ISO 14001 para medio ambiente, etc.).

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

- ***Alcance del SGSI:*** ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGS considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

- ***Política y objetivos de seguridad***: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

- ***Procedimientos y mecanismos de control que soportan al SGSI:*** aquellos procedimientos que regulan el propio funcionamiento del SGSI. Documentación necesaria para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados -Métricas.

- ***Enfoque de evaluación de riesgos:*** descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables .

- ***Informe de evaluación de riesgos:*** estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

- ***Plan de tratamiento de riesgos:*** documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

- ***Procedimientos documentados:*** todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

- ***Registros:*** documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

- ***Declaración de aplicabilidad:*** (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

6.5.5.1 Control de la documentación

Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

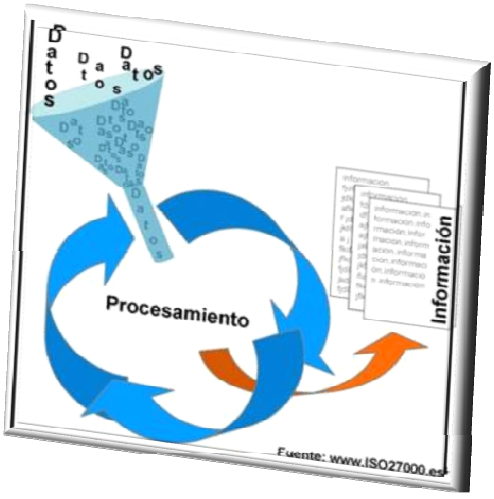


Fig. F.13 Procesamiento de la información - Fuente: www.ISO27000.es

•Aprobar documentos apropiados antes de su emisión.
• Revisar y actualizar documentos cuando sea necesario y renovar su validez.
• Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
• Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
• Garantizar que los documentos se mantienen legibles y fácilmente identificables.
• Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
• Garantizar que los documentos procedentes del exterior están identificados.
• Garantizar que la distribución de documentos está controlada.
• Prevenir la utilización de documentos obsoletos.
• Aplicar la identificación

6.5.5.2 ¿Cómo se implementa un SGSI?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

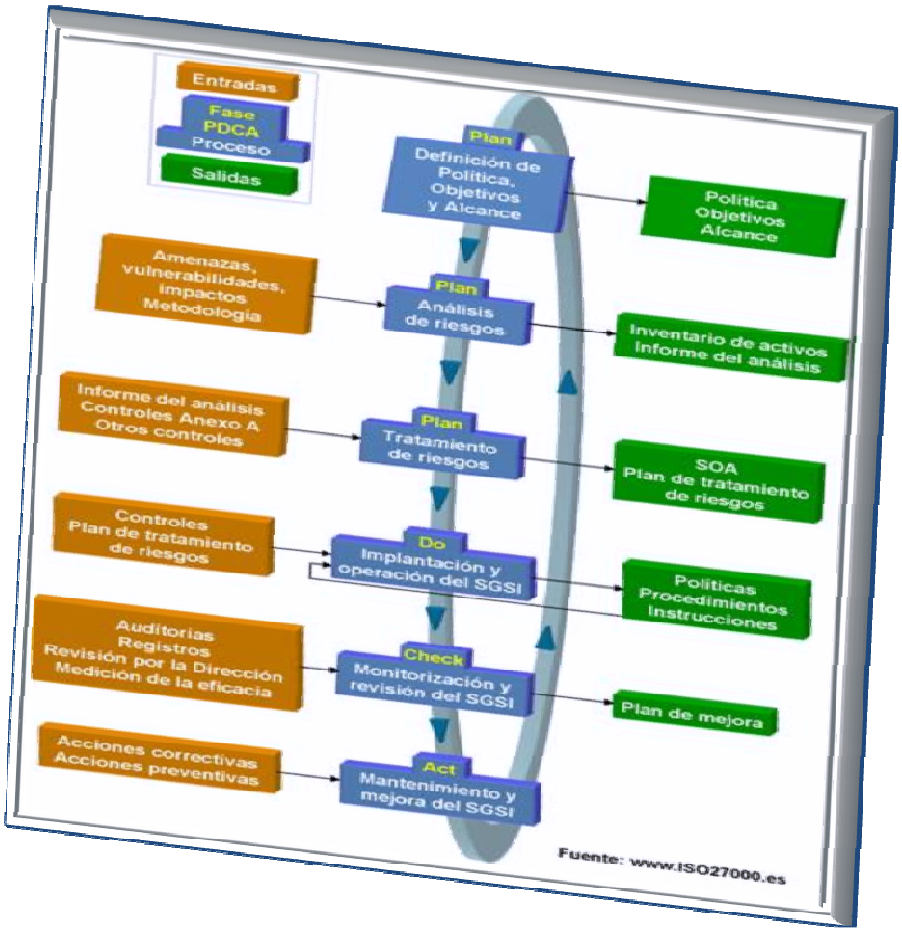


Fig. F.14 Plan-Do-Check-Act – Fuente: www.ISO27000.es

• ***Plan (planificar):*** establecer el SGSI.

• ***Do (hacer):*** implementar y utilizar el SGSI.

• ***Check (verificar):*** monitorizar y revisar el SGSI.

• ***Act (actuar):*** mantener y mejorar el SGSI

6.5.5.2.1 Plan: Establecer el SGSI

• Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

• Definir una política de seguridad que:

– Incluya el marco general y los objetivos de seguridad de la información de la organización;

– Considere requerimientos legales o contractuales relativos a la seguridad de la información;

– Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI.
– Establezca los criterios con los que se va a evaluar el riesgo;

– Esté aprobada por la dirección.

• Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia).

• Identificar los riesgos:
– Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios.

– Identificar las amenazas en relación a los activos;

– Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.

– Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

• Analizar y evaluar los riesgos:
– Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información.

– Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados.

– Estimar los niveles de riesgo.
– Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

• Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:
– Aplicar controles adecuados.

– Aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos.

– Evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan.

– Transferir el riesgo a terceros, p. ej., compañías aseguradoras o proveedores de outsourcing.

• Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.

• Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.

• Definir una declaración de aplicabilidad que incluya:
– Los objetivos de control y controles seleccionados y los motivos para su elección.

– Los objetivos de control y controles que actualmente ya están implantados.

– Los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

Fig. F.15 Gestión de Riesgos Fuente: www.ISO27000.es

En relación a los controles de seguridad, el estándar ISO 27002 (antigua ISO 17799) proporciona una completa guía de implantación que contiene 133 controles, según 39 objetivos de control agrupados en 11 dominios. Esta norma es referenciada en ISO 27001, en su segunda cláusula, en términos de "documento indispensable para la aplicación de este documento" y deja abierta la posibilidad de incluir controles adicionales en el caso de que la guía no contemplase todas las necesidades particulares.

6.5.5.2.2 Do: Implementar y utilizar el SGSI

• Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

• Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

• Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.

• Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.

• Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.

• Gestionar las operaciones del SGSI.

• Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.

• Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

6.5.5.2.3 Check: Monitorizar y revisar el SGSI

La organización deberá:

• Ejecutar procedimientos de monitorización y revisión para:

– Detectar a tiempo los errores en los resultados generados por el procesamiento de la información.

– Identificar brechas e incidentes de seguridad.

– Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto.

– Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores.

– Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

• Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

• Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

• Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.-.

• Realizar periódicamente auditorías internas del SGSI en intervalos planificados.

• Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.

• Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.

• Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

6.5.5.2.4 Act: Mantener y mejorar el SGSI

La organización deberá regularmente:
• Implantar en el SGSI las mejoras identificadas.
• Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.

• Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.

• Asegurarse que las mejoras introducidas alcanzan los objetivos previstos. PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases.

Téngase en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, p. ej., puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

Este estándar es certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo, puede solicitar una auditoría externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

6.5.5.3 ¿Qué tareas tiene la Gerencia en un SGSI?

Uno de los componentes primordiales en la implantación exitosa de un Sistema de Gestión de Seguridad de la Información es la implicación de la dirección. No se trata de una expresión retórica, sino que debe asumirse desde un principio que un SGSI afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y

acciones que sólo puede tomar la gerencia de la organización. No se debe caer en el error de considerar un SGSI una mera cuestión técnica o tecnológica relegada a niveles inferiores del organigrama; se están gestionando riesgos e impactos de negocio que son responsabilidad y decisión de la dirección.

El término Dirección debe contemplarse siempre desde el punto de vista del alcance del SGSI. Es decir, se refiere al nivel más alto de gerencia de la parte de la organización afectada por el SGSI (recuérdese que el alcance no tiene por qué ser toda la organización).
Algunas de las tareas fundamentales del SGSI que ISO 27001 asigna a la dirección se detallan en los siguientes puntos:

6.5.5.3.1 Compromiso de la dirección

La dirección de la organización debe comprometerse con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. Para ello, debe tomar las siguientes iniciativas:

• Establecer una política de seguridad de la información.

• Asegurarse de que se establecen objetivos y planes del SGSI.

• Establecer roles y responsabilidades de seguridad de la información.

• Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.

• Asignar suficientes recursos al SGSI en todas sus fases.

• Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.

• Asegurar que se realizan auditorías internas.

• Realizar revisiones del SGSI, como se detalla más adelante.

6.5.5.3.2 Asignación de recursos

Para el correcto desarrollo de todas las actividades relacionadas con el SGSI, es imprescindible la asignación de recursos. Es responsabilidad de la dirección garantizar que se asignan los suficientes para:

• Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI.

• Garantizar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio.

• Identificar y tratar todos los requerimientos legales y normativos, así como las obligaciones contractuales de seguridad.

• Aplicar correctamente todos los controles implementados, manteniendo de esa forma la seguridad adecuada.

• Realizar revisiones cuando sea necesario y actuar adecuadamente según los resultados de las mismas.

• Mejorar la eficacia del SGSI donde sea necesario.

6.5.5.3.3 Formación y concienciación

La formación y la concienciación en seguridad de la información son elementos básicos para el éxito de un SGSI. Por ello, la dirección debe asegurar que todo el personal de la organización al que se le asignen responsabilidades definidas en el SGSI esté suficientemente capacitado. Se deberá:

• Determinar las competencias necesarias para el personal que realiza tareas en aplicación del SGSI.

• Satisfacer dichas necesidades por medio de formación o de otras acciones como, p. ej., contratación de personal ya formado.

• Evaluar la eficacia de las acciones realizadas.

• Mantener registros de estudios, formación, habilidades, experiencia y cualificación.
Además, la dirección debe asegurar que todo el personal relevante este concienciado de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI.

6.5.5.3.4 Revisión del SGSI

A la dirección de la organización se le asigna también la tarea de, al menos una vez al año, revisar el SGSI, para asegurar que continúe siendo adecuado y eficaz. Para ello, debe recibir una serie de informaciones, que le ayuden a tomar decisiones, entre las que se pueden enumerar:

• Resultados de auditorías y revisiones del SGSI.

• Observaciones de todas las partes interesadas.

• Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.

• Información sobre el estado de acciones preventivas y correctivas.

• Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.

• Resultados de las mediciones de eficacia.

• Estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección.

• Cualquier cambio que pueda afectar al SGSI.

• Recomendaciones de mejora.

Basándose en todas estas informaciones, la dirección debe revisar el SGSI y tomar decisiones y acciones relativas a:

- Mejora de la eficacia del SGSI.

- Actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.

- Modificación de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.

- Necesidades de recursos.

- Mejora de la forma de medir la efectividad de los controles.

6.5.5.3.5 Arranque del proyecto

• ***Compromiso de la Dirección:***
Una de las bases fundamentales sobre las que iniciar un proyecto de este tipo es el apoyo claro y decidido de la Dirección de la organización. No sólo por ser un punto contemplado de forma especial por la norma sino porque el cambio de cultura y concienciación que lleva consigo el proceso hacen necesario el impulso constante de la Dirección.

• ***Planificación, fechas, responsables***:
Como en todo proyecto de envergadura, el tiempo y el esfuerzo invertidos en esta fase multiplican sus efectos positivos sobre el resto de fases.

Planificación.-

• ***Definir alcance del SGSI:***
En función de características del negocio, organización, localización, activos y tecnología, definir el alcance y los límites del SGSI (el SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado.

• ***Definir política de seguridad:***
Que incluya el marco general y los objetivos de seguridad de la información de la organización, tenga en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad, esté alineada con la gestión de riesgo general, establezca criterios de evaluación de riesgo y sea aprobada por la Dirección. La política de seguridad es un documento muy general, una especie de "declaración de intenciones" de la Dirección, por lo que no pasará de dos o tres páginas.

• ***Definir el enfoque de evaluación de riesgos:***
Definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente (ver sección de Herramientas); la organización

puede optar por una de ellas, hacer una combinación de varias o crear la suya propia. ISO 27001 no impone ninguna ni da indicaciones adicionales sobre cómo definirla (en el futuro, ISO 27005 proporcionará ayuda en este sentido). El riesgo nunca es totalmente eliminable -ni sería rentable hacerlo-, por lo que es necesario definir una estrategia de aceptación de riesgo.

• ***Inventario de activos:***
Todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.

• ***Identificar amenazas y vulnerabilidades:***
Todas las que afectan a los activos del inventario.

• ***Identificar los impactos:***
Los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.

• ***Análisis y evaluación de los riesgos:***
Evaluar el daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad) y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.

• ***Identificar y evaluar opciones para el tratamiento del riesgo:***
El riesgo puede reducido (mitigado mediante controles), eliminado (p. ej., eliminando el activo), aceptado (de forma consciente) o transferido (p. ej., con un seguro o un contrato de outsourcing).

• ***Selección de controles:***
Seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001 (teniendo en cuenta que las exclusiones habrán de ser justificadas) y otros controles adicionales si se consideran necesarios.

• ***Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI:***
Hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).

• ***Confeccionar una Declaración de Aplicabilidad:***
La llamada SOA (Statement of Applicability) es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

Implementación.-

• Definir plan de tratamiento de riesgos:
Que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

• Implantar plan de tratamiento de riesgos:
Con la meta de alcanzar los objetivos de control identificados.

• Implementar los controles:
Todos los que se seleccionaron en la fase anterior.

• Formación y concienciación:
De todo el personal en lo relativo a la seguridad de la información.

• Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.

• Gestionar las operaciones del SGSI y todos los recursos que se le asignen.

• Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

Seguimiento.-

• Ejecutar procedimientos y controles de monitorización y revisión:
Para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado, detectar y prevenir incidentes de seguridad mediante el uso de indicadores y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.

• Revisar regularmente la eficacia del SGSI:
En función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y feedback de todos los interesados.

• Medir la eficacia de los controles:
Para verificar que se cumple con los requisitos de seguridad.

• Revisar regularmente la evaluación de riesgos:
Los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.

• Realizar regularmente auditorías internas:
Para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.

• ***Revisar regularmente el SGSI por parte de la Dirección:***
Para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.

• ***Actualizar planes de seguridad:***
Teniendo en cuenta los resultados de la monitorización y las revisiones.

• ***Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI:***
Sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

Mejora continua.-

• ***Implantar mejoras:***
Poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.

• ***Acciones correctivas:***
Para solucionar no conformidades detectadas.

• ***Acciones preventivas:***
Para prevenir potenciales no conformidades.

• ***Comunicar las acciones y mejoras:***
A todos los interesados y con el nivel adecuado de detalle.

• ***Asegurarse de que las mejoras alcanzan los objetivos pretendidos:***
La eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

Aspectos Clave.-

• Compromiso y apoyo de la Dirección de la organización.
• Definición clara de un alcance apropiado.
• Concienciación y formación del personal.
• Evaluación de riesgos exhaustiva y adecuada a la organización.
• Compromiso de mejora continua.
• Establecimiento de políticas y normas.
• Organización y comunicación.
• Integración del SGSI en la organización.

Factores de éxito.-

• La concienciación del empleado por la seguridad. Principal objetivo a conseguir.
• Realización de comités de dirección con descubrimiento continuo de no conformidades o acciones de mejora.
• Creación de un sistema de gestión de incidencias que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).
• La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.
• La seguridad no es un producto, es un proceso.

• La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.
• La seguridad debe ser inherente a los procesos de información y del negocio.

Riesgos.-

• Exceso de tiempos de implantación: con los consecuentes costes descontrolados, desmotivación, alejamiento de los objetivos iniciales, etc.
• Temor ante el cambio: resistencia de las personas.
• Discrepancias en los comités de dirección.
• Delegación de todas las responsabilidades en departamentos técnicos.
• No asumir que la seguridad de la información es inherente a los procesos de negocio.
• Planes de formación y concienciación inadecuados.
• Calendario de revisiones que no se puedan cumplir.
• Definición poco clara del alcance.
• Exceso de medidas técnicas en detrimento de la formación, concienciación y medidas de tipo organizativo.
• Falta de comunicación de los progresos al personal de la organización.

Consejos básicos.-

• ***Mantener la sencillez y restringirse a un alcance manejable y reducido:***
Un centro de trabajo, un proceso de negocio clave, un único centro de proceso de datos o un área sensible concreta; una vez conseguido el éxito y observados los beneficios, ampliar gradualmente el alcance en sucesivas fases.

• ***Comprender en detalle el proceso de implantación***:
Iniciarlo en base a cuestiones exclusivamente técnicas es un error frecuente que rápidamente sobrecarga de problemas la implantación; adquirir experiencia de otras implantaciones, asistir a cursos de formación o contar con asesoramiento de consultores externos especializados.

• Gestionar el proyecto fijando los diferentes hitos con sus objetivos y resultados.

• La autoridad y compromiso decidido de la Dirección de la empresa:
Incluso si al inicio el alcance se restringe a un alcance reducido- evitarán un muro de excusas para desarrollar las buenas prácticas, además de ser uno de los puntos fundamentales de la norma.

• ***La certificación como objetivo:***
Aunque se puede alcanzar la conformidad con la norma sin certificarse, la certificación por un tercero asegura un mejor enfoque, un objetivo más claro y tangible y, por lo tanto, mejores opciones de alcanzar el éxito.

• ***No reinventar la rueda:***
Aunque el objetivo sea ISO 27001, es bueno obtener información relativa a la gestión de la seguridad de la información de otros métodos y marcos reconocidos.

• ***Servirse de lo ya implementado:***
Otros estándares como ISO 9001 son útiles como estructura de trabajo, ahorrando tiempo y esfuerzo y creando sinergias; es conveniente pedir ayuda e implicar a auditores internos y responsables de otros sistemas de gestión.

• ***Reservar la dedicación necesaria diaria o semanal:***
El personal involucrado en el proyecto debe ser capaz de trabajar con continuidad en el proyecto.

• ***Registrar evidencias:***
Deben recogerse evidencias al menos tres meses antes del intento de certificación para demostrar que el SGSI funciona adecuadamente.

6.5.5.4 ¿En qué ayudan los sistemas de gestión en general?

Aseguran que una organización es dirigida de un modo eficiente y eficaz.
Formalizan y sistematizan la gestión en procedimientos escritos, instrucciones, formularios y registros que aseguren la eficiencia de la organización y su mejora continua.

¿Qué información protege un SGSI?

Los activos de información de una organización, independientemente del soporte que se encuentren; p. ej., correos electrónicos, informes, escritos relevantes, páginas web, imágenes, documentos, hojas de cálculo, faxes, presentaciones, contratos, registros de clientes, información confidencial de trabajadores y colaboradores.

¿Qué es exactamente la seguridad de la información?

La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la misma y de los sistemas implicados en su tratamiento dentro de una organización. Estos tres factores se definen como:
• Confidencialidad: acceso a la información por parte únicamente de quienes estén autorizados.
• Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
• Disponibilidad: acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.
Tengo un firewall, actualizo regularmente el antivirus y realizo copias de backup.

¿Qué aporta un SGSI a mi empresa?

Estas medidas no son más que unos pocos controles técnicos que, por sí mismos, no significan que se esté gestionando la seguridad. Un SGSI implica que la organización ha estudiado los riesgos a los que está sometida toda su información, ha evaluado qué nivel de riesgo asume, ha implantado controles (no sólo tecnológicos, sino también organizativos) para aquellos riesgos que superan dicho nivel, ha documentado las

políticas y procedimientos relacionados y ha entrado en un proceso continuo de revisión y mejora de todo el sistema.
El SGSI da así la garantía a la empresa de que los riesgos que afectan a su información son conocidos y gestionados. No se debe olvidar, por tanto, que no hay seguridad total sino seguridad gestionada.

¿Existe algún producto que cubra los principales aspectos de seguridad de la información?

No. Por influencia de la publicidad y las campañas de venta agresivas, es un error común pensar que el nivel de seguridad depende exclusivamente del presupuesto dedicado a la compra de productos relacionados.

La seguridad exige de un plan de gestión del riesgo continuado, políticas adecuadas a cada empresa y una seguridad establecida en base a múltiples y diferentes barreras. Siempre hay que recordar que la seguridad no es un producto sino un proceso.

Si la seguridad total no existe, ¿qué diferencia aporta un SGSI?

Un SGSI es el modo más eficaz de conseguir minimizar los riesgos, asegurar la continuidad adecuada de las actividades de negocio hasta en los casos más extremos y de adaptar la seguridad a los cambios continuos que se producen en la empresa y en su entorno. Aunque nunca logremos la seguridad total, nos acercamos a ella mediante una

mejora continua. Es más apropiado hablar en términos de riesgo asumible en lugar de seguridad total, ya que no sería lógico que el gasto en seguridad sea mayor que los impactos potenciales de los riesgos que pretende evitar.

¿En qué consiste la gestión del riesgo y el ciclo de vida PDCA?

Mediante la gestión del riesgo se identifican, evalúan y corrigen a niveles razonables y asumibles en coste todos los riesgos en seguridad que podrían afectar a la información.
PDCA son las siglas en inglés del conocido como ciclo de Deming: Plan-Do-Check-Act (Planificar-Hacer-Verificar-Actuar).

En la fase PLAN se realiza la evaluación de las amenazas, riesgos e impactos.

En la fase DO, se seleccionan e implementan los controles que reduzcan el riesgo a los niveles considerados como aceptables y en CHECK y ACT se cierra y reinicia el ciclo de vida con la recogida de evidencias y readaptación de los controles según los nuevos niveles obtenidos y requeridos.

Es un proceso cíclico sin fin que permite la mejor adaptación de la seguridad al cambio continuo que se produce en la empresa y su entorno.

6.5.5.5 Certificación

¿Por qué dentro de la serie es certificable únicamente la 27001?

Es la norma que define el modelo completo de gestión de seguridad de la información según ciclo PDCA aunque, para algunos procesos, se apoya en otras normas relacionas no certificables, como ISO 27002.

¿Quién certifica a mi empresa en ISO 27001?

Una entidad de certificación acreditada, mediante una auditoría. Esta entidad establece el número de días y auditores necesarios, puede realizar una pre auditoria (no obligatoria) y lleva a cabo una auditoría formal. Si el informe es favorable, la empresa recibirá la certificación.
Para mayor detalle, consulte nuestra sección de Certificación (http://www.iso27000.es/certificacion.html).

¿En qué ayuda a las empresas la auditoría de certificación?

Supone la oportunidad de recibir la confirmación por parte de un experto ajeno a la empresa de que se está gestionando correctamente la seguridad de la información.
Añade un factor de tensión y de concentración en un objetivo a todos los miembros del proyecto y de la organización en general, lo que redunda en beneficio de la implantación del sistema. Da una señal al mercado de que la empresa en cuestión es confiable y es gestionada transparentemente.
Es el requisito indispensable para acceder a la certificación y poder utilizar el sello de certificación junto al de la propia empresa.
Esta condición será muy favorable al entablar futuras relaciones laborales con demás empresas

¿Por qué crece el número de empresas certificadas?

El acta Sarbanes-Oxley en EEUU y la publicación de directivas en el ámbito EU y en cada estado miembro ha activado las alarmas en la dirección de las empresas. Adicionalmente a los requisitos legales establecidos para auditorías financieras, gestión de riesgos, financiación, plan de desastres, continuidad de negocio, etc., crece el número de requisitos legales relacionados con la protección de los datos de carácter personal.
ISO27001 ayuda a considerar y adoptar los controles necesarios en los procesos de negocio y tratamiento de la información para satisfacer las demandas de la empresa, legales y de los clientes en materia de seguridad de la información.

¿Obliga mi certificación a la de mis empresas de servicio externas (outsourcing)?

No necesariamente. ISO27001 indica los controles a considerar para servicios de outsourcing desde el ámbito de su empresa (requisitos contractuales, niveles de servicio, obligaciones legales, auditoría, etc.). La seguridad de los sistemas de información que

están fuera del ámbito es responsabilidad de la empresa externa, que debe cumplir regularmente con los compromisos contractuales exigidos por el cliente.

¿Dónde puedo ver si una empresa está certificada?

El registro oficial de organizaciones certificadas en ISO 27001 o BS 7799-2 a nivel mundial está en http://www.iso27001certificates.com.

¿Quién acredita a las entidades certificadoras?

Cada país tiene una entidad de acreditación (algunos, varias) que se encarga de supervisar que las entidades de certificación (las que, finalmente, auditan y certifican los sistemas de gestión de las empresas) están capacitadas para desempeñar su labor y se ajustan a los esquemas establecidos. En España, es ENAC (Entidad Nacional de Acreditación; http://www.enac.es) quien tiene esta misión.
También se da el caso de entidades certificadoras que expiden certificados bajo esquema de acreditación de una entidad de acreditación extranjera. En ISO 27001, se da frecuentemente el caso con UKAS (entidad nacional de acreditación del Reino Unido), por el origen inglés de la norma y su corta vida aún como ISO.

¿Cómo es el proceso de certificación?

El proceso de certificación puede resumirse en las siguientes fases:
• Solicitud por parte del interesado a la entidad de certificación y toma de datos por parte de la misma.
• Respuesta en forma de oferta por parte de la entidad certificadora.
• Compromiso.

• Designación de auditores, determinación de fechas y establecimiento conjunto del plan de auditoría.
• Pre-auditoría: opcionalmente, puede realizarse una auditoría previa que aporte información sobre la situación actual y oriente mejor sobre las posibilidades de superar la auditoría real.
• Fase 1 de la auditoría: revisión del alcance, política de seguridad, Dirección, análisis de riesgos, declaración de aplicabilidad y procedimientos clave.
• Fase 2 de la auditoría: revisión de las políticas, auditoría de la implantación de los controles de seguridad y verificación de la efectividad del sistema.
• Certificación: acciones correctivas en caso de no conformidades graves, revisión y emisión de certificado en caso de informe favorable.
• Auditoría de seguimiento: auditoría semestral o anual de mantenimiento.
• Auditoría de re-certificación: cada tres años, una auditoría de certificación formal completa.

¿Alguien puede obligarme a certificarme en ISO 27001?

Como obligación legal, a día de hoy, no. Sin embargo, como en toda relación comercial, el cliente puede exigir a su proveedor ciertas condiciones previas para ser considerado siquiera como opción de contratación.
Hay administraciones públicas que están empezando a exigir certificados de este tipo a las empresas que quieran acceder a concursos públicos de productos o servicios relacionados con sistemas de información. Igualmente, es previsible que empresas privadas comiencen en algún momento a exigírselo a sus proveedores siempre que vaya a haber algún tipo actividad relacionada con información sensible.
Lista de términos relacionados con la serie ISO 27000 y la seguridad de la información, definidos en el contexto de las mismas. Se incluye la correspondencia en inglés de cada uno de los términos.

6.6 ANEXO VI

6.6.1 Glosario

6.6.1.1 Glosario de Términos

En este glosario se presentan los términos de uso frecuente en el entorno del análisis de riesgos.

En la elaboración de este glosario se han obtenido en cuenta las definiciones recogidas en los principales estándares que se detallan en la Norma Iso-27000

Activo.- En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.

Alcance.- Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Amenaza.- Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de impacto al negocio: evaluar los resultados y las consecuencias de la inestabilidad.

Análisis de riesgos.- Según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Autorización: Lo que se permite cuando se ha otorgado acceso.

Confidencialidad.- Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad. La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.

Control.- Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

Control de Acceso: limitar el acceso autorizado solo a entidades autenticadas.

Disponibilidad.- Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizada para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La Alta disponibilidad sistemas objetivo debe seguir estando disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema. Garantizar la disponibilidad implica también la prevención de ataque Denegación de servicio. La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera, tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web etc., mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

Evaluación de riesgos.- Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento.- Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

Gestión de riesgos.- Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Identificación: verificación de una persona o cosa; reconocimiento.

IEC.- Organización internacional que publica estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas.

Impacto.- El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.-.

Incidente.- Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad.- Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. No es igual a integridad referencial en bases de datos. La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital Es uno de los pilares fundamentales de la seguridad de la información.

ISO 27001.- Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005

Objetivo.- Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

PDCA. - Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

Políticas: declaración de alto nivel sobre la intención y la dirección de la gerencia.

Política de seguridad.- Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.

Riesgo.- Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Residual.- Según [ISO/IEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

Seguridad de la información.- Según [ISO/IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

SGSI.- Sistema de Gestión de la Seguridad de la Información. Según [ISO/IEC 27001:2005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Tratamiento de riesgos.- Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

Valoración de riesgos.- Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Vulnerabilidad.- Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

6.6.1.2 Glosario de Abreviaturas

CID: Acrónimo español de confidencialidad, integridad y disponibilidad, los parámetros básicos de la seguridad de la información.

IEC: International Electrotechnical Commission.

ISMS: Information Security Management System, Sistema de Gestión de Seguridad de la información.

ISO: International Organization for Standarization, Organización Internacional de Estandarización.

PDCA: Plan, Do, Check, Act. Planificar, Ejecutar, Comprobar, Actuar. Ciclo de Deming o de la mejora continua.

SGSI: Sistema de Gestión de Seguridad de la Información.