



ESCUELA SUPERIOR POLITECNICA DEL  
LITORAL

CENTRO DE EDUCACION CONTINUA

**DIPLOMADO EN AUDITORIA INFORMATICA**

**I PROMOCION**

**“SISTEMA DE GESTIÓN DE SEGURIDAD  
DE LA INFORMACIÓN  
PARA EL SISTEMA HOSPITALARIO DOCENTE DE LA  
UNIVERSIDAD DE GUAYAQUIL”**

**PARTICIPANTES:  
ING. ANGELICA AGUIAR A.  
ING. SISIANA CHAVEZ CH.  
ING. LUIS DIER L.**

**2006**

# INDICE

<b>ABSTRACTO</b>	<b>1</b>
<b>CAPITULO1: INTRODUCCION</b>	
1.1 Que es la seguridad de la Información	3
1.2 Necesidad de Gestionar la seguridad de Información	5
1.3 Objetivos de la Seguridad de la Información	6
1.3.1 La Integridad de la información	7
1.3.2 La disponibilidad u Operatividad	7
1.3.3 La privacidad o confidencialidad	7
1.3.4 La autenticidad	8
1.3.5 Protección a la Réplica	8
1.3.6 No repudio	8
1.4 Situación Actual en Seguridades	9
1.4.1 Activos	9
1.4.2 Recursos de Información	9
1.4.3 Recursos de Software	10
1.4.4 Activos físicos	10
1.4.5 Servicios	10
1.5 Vulnerabilidades	11
1.6 Amenazas a la Seguridad	12
1.7 Riesgo y Control	12
1.8 Impacto	12
1.9 Probabilidad	12
1.10 Análisis de Riesgos	13
1.10.1 Como protegerlo?	13
1.10.2 Disponibilidad	13
1.10.3 Integridad	14
1.10.4 Confidencialidad	14
1.11 Tipos de Amenazas de Seguridad	14
1.12 Objetivo de un SGSI	15
1.13 Responsabilidades de un SGSI	15
1.14 Apoyo Político	16
1.15 Gasto o Inversión	17

## **CAPITULO 2: \_SISTEMA HOSPITALARIO DOCENTE**

2.1	Antecedentes	<b>18</b>
2.2	Reseña Histórica	18
2.3	SHDUG Atención al público	19
2.3.1	Docencia e Investigación	19
2.3.2	Gineco-Obstetrica-Perinatólogica	19
2.3.3	Hospital de Especialidades	19
2.4	Visión	20
2.5	Misión	20
2.6	Objetivos	21

## **CAPITULO 3: MARCO CONCEPTUAL DE DESARROLLO**

3.1	Marco Conceptual de Desarrollo	<b>22</b>
3.2	Porque COBIT ?	23
3.3	Porque COBIT y no ISO 17799?	23
3.4	Usuarios de COBIT	25
3.5	Descripción de Dominios de COBIT	26
3.6	Marco Referencial	27
3.7	Modelo de Madurez para autoevaluación	30
3.8	Niveles de Madurez de la Administración de Riesgos	30
3.9	Representación gráfica del Modelo de Madurez	32
3.10	Evaluación de Riesgos	32
3.10.1	Valoración del Riesgo	32
3.10.2	Identificación del Riesgo	32
3.10.3	Análisis del Riesgo	33
3.10.4	Probabilidad	33
3.10.5	Impacto	33
3.10.6	Priorización de los Riesgos	34
3.10.7	Determinación del nivel de Riesgo	34

## **CAPITULO 4: METODOLOGIA DE DESARROLLO DE TRABAJO**

4.1	Selección de Objetivos de Control	<b>36</b>
4.2	Nivel de Madurez	36

4.3	Objetivos Primarios para Sistema Hospitalario	36
4.4	Conclusiones de Priorización	37
4.5	Análisis de Riesgo	38
4.5.1	Determinación del nivel de riesgo	38
4.5.2	Evaluación de Controles Existentes	58

## **CAPITULO 5:\_POLITICAS GENERALES DE SEGURIDAD**

5.1	Generalidades	<b>71</b>
5.2	Objetivo	72
5.3	Alcance	72
5.4	Responsabilidad	72
5.4.1	Persona encargada de la Seguridad	72
5.4.2	Gerente de Área de Tecnología	73
5.4.3	Propietarios de la Información	73
5.4.4	Coordinador de Recursos Humanos	73
5.4.5	Responsable del Area Legal	73
5.4.6	Usuarios de la Información	73
5.5	Objetivo	75
5.6	Alcance	75
5.7	Responsabilidad	76
5.8	Política Inventario de Activos	76
5.9	Clasificación de la Información	77
5.10	Rotulado de la Información	78
5.11	Plan de Aplicabilidad	79

## **CAPITULO 6:\_POLITICAS ESPECIFICAS**

6.1	Control de Accesos	<b>87</b>
6.1.1	Generalidades	87
6.1.2	Objetivos	87
6.1.3	Alcance	88
6.1.4	Responsabilidad	88
6.2	Política de Control de Accesos	91
6.2.1	Reglas de Control de Accesos	91
6.2.2	Administración de Accesos de Usuarios	91
6.2.3	Registro de Usuarios	94

6.2.4	Administración de Privilegios	94
6.2.5	Administración de Contraseñas de Usuario	95
6.2.6	Administración de Contraseñas Críticas	96
6.2.7	Revisión de Derechos de Usuarios	97
6.2.8	Responsabilidades del Usuario	98
6.3	Seguridad Física y Ambiental	100
6.3.1	Generalidades	100
6.3.2	Objetivos	101
6.3.3	Alcance	101
6.3.4	Responsabilidad	101
6.4	Política Perímetro de Seguridad Física	102
6.4.1	Controles de Acceso Físico	104
6.4.2	Protección de Oficinas e Instalaciones	105
6.4.3	Desarrollo de Tareas en Áreas Protegidas	106
6.4.4	Aislamiento de las Áreas de Recepción y Distribución	107
6.4.5	Ubicación y Protección del equipamiento	108
6.4.6	Suministros de Energía	109
6.4.7	Seguridad del Cableado	110
6.4.8	Mantenimiento de Equipos	111
6.4.9	Seguridad de los Equipos fuera de Instalaciones	111
6.4.10	Reutilización Segura de los equipos	112
6.5	Políticas de Escritorios y Pantallas Limpias	112
6.6	Política de Retiro de los Bienes	114
	<b>CONCLUSIONES GENERALES</b>	<b>114</b>
	<b>GLOSARIO</b>	<b>117</b>
	<b>BIBLIOGRAFÍA</b>	<b>122</b>
	<b>ANEXOS</b>	
	<b>A:</b> Situación Actual de la Empresa	123
	<b>B:</b> Selección de Procesos y Objetivos de Control	139

## **ABSTRACTO**

En este documento contiene el diseño de un Sistema de Gestión de Seguridad de la Información para el Sistema Hospitalario Docente Universitario, el cual se encuentra dividido en 6 capítulos . A continuación una breve descripción de estos.

En el primer capítulo tenemos la introducción sobre que es un sistema de gestión de seguridad de la información para poder lograr un entendimiento global sobre la importancia de la seguridad de la información, criterios que la identifican, conceptos actuales, cuales son sus riesgos, etc.

En el segundo capítulo nos muestra información del Hospital Universitario como es su historia, misión, visión, valores y objetivos, esto nos ayuda a entender el negocio que es muy importante para luego ir identificando donde es necesario proteger la información y donde la tecnología nos ayudaría a ir cumpliendo los objetivos del negocio y como aportarle valor adicional a lo que se tiene actualmente.

En el tercer capítulo se da a conocer el marco conceptual que se escogió para realizar el diseño del sistema de gestión de seguridad , aquí se indicará porque se lo escogió , de que se trata este marco referencial y todas las herramientas que nos provee para poder realizar nuestro trabajo y como se lo puede aplicar

En el cuarto capítulo se indica la metodología o los pasos que se siguieron para llegar a realizar el diseño, se muestra en detalle el trabajo realizado, todo lo que se elaboro en base al marco referencial escogido por sus buenas practicas como son la matriz de riesgos e impactos, selección de criterios, pruebas de controles.

Y en el capítulo cinco se muestra las políticas generales de seguridad creadas para el Hospital Universitario y su plan de aplicabilidad basadas en las pruebas de diseño de controles que nos identifican cuales son sus amenazas, vulnerabilidades, áreas mas criticas, etc , políticas creadas para proteger la información ,tener una concientización con respecto a seguridad y riesgos ya que estas son hechas para que sean aplicadas por todos los empleados.

Y por último en el capítulo 6 vemos ya políticas específicas que han sido mejoradas o añadidas de acuerdo a las pruebas de controles que se realizaron así como sus pruebas de efectividad y el plan de aplicabilidad que se tiene para la implementación del diseño que se realizó del sistema de gestión de seguridad de la información para el Hospital Universitario, estas políticas no serán siempre estables, deberán a través del tiempo ser actualizadas, mejoradas, aumentadas, algunas eliminadas, etc ya que el avance de la tecnología nos traerá otros riesgos y de pronto las políticas que teníamos ya no nos ayudarán a mejorar nuestro nivel de seguridad o en todo caso siempre deberá hacerse una revisión de éstas así como también velar porque se cumplan.

## **CAPITULO 1.- INTRODUCCIÓN**

En otros tiempos la seguridad de la información era fácilmente administrable, solo bastaba con resguardar los documentos mas importantes bajo llave y mantener vigilados a los empleados que poseían algo de conocimientos, poniendo guardias de seguridad. Los sistemas de computación entraron en las oficinas y obligaron a los sistemas de seguridad a evolucionar para poder mantenerse al día con la tecnología cada día cambiante.

De manera similar otros delitos fueron apareciendo, cuantificar los gastos y las perdidas en seguridad de la información o delitos informáticos era prácticamente imposible, si bien se tiende a minimizar los riesgos, este nunca desaparece, por otro lado el objetivo principal de la seguridad es proteger los sistemas informáticos de tal manera que se garantiza la disponibilidad, integridad y confiabilidad de la información, además de preservar su uso para beneficio de la organización.

En nuestro país algunas instituciones se han visto sujeta a los ataques en sus instalaciones, tanto desde el interior como del exterior, basta decir que estamos sujetos a formar grupos de personas que se involucran y están pendientes, tratando de contrarrestar y anular estas amenazas reales, las cuales cuando ocurren no son divulgadas.

Ejemplos de hechos acontecidos en nuestro país son entre ellos; en un importante Banco de la localidad donde el Departamento de Seguridad descubrió un mecanismo mediante el cual se depositaban en una cuenta determinada cantidad de centavos de diferencia en el calculo de intereses en tarjetas de crédito, aparentemente decimos centavos y esto puede que no parezca un delito pero multipliquemos esos centavos por el volumen de transacciones que maneja un banco y eso por el numero de días durante los que se realizo el delito, el resultado una gran cantidad de dinero.

Las estadísticas nos indican que las empresas no solo en Latinoamérica, sino en el mundo entero, están orientando su enfoque hacia procesos de seguridad, los gerentes están destinando parte de su presupuesto anual a inversiones relacionadas con seguridad, sea esta en cualquiera de sus formas: seguridad lógica, seguridad física, ataques externos, compra de equipos de detección de intrusos, etc.



Esto es comprensible ya que no es deseable que se conozcan que los sistemas no son seguros, ya que generaría, desconfianza en sus clientes o proveedores en otras palabras es una desventaja tanto estratégica como competitiva.

En otros países la seguridad de las instituciones se ha convertido en cuestión de seguridad nacional, por ello contar con un documento de políticas de seguridad es imprescindible, y debe de plasmar mecanismos confiables que con base en la política institucional proteja los activos de la institución.

El objetivo principal de la Gestión de Seguridad de la Información es brindar a los usuarios de los recursos informáticos, con la cantidad y calidad que demandan, esto es, que tengamos continuidad del servicio los 365 días del año, de forma confiable. Así, la cantidad de recursos de computación y de telecomunicaciones con que cuenta la institución son de consideración y se requiere que se protejan para garantizar su buen funcionamiento, así como salvaguardar la información que estos manejan.

### **1.1.- ¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?**

La información es uno de los recursos principales de las organizaciones. ¿Piense que pasaría si roban la fórmula de algún producto muy conocido de gran aceptación internacional? ¿Cuánto representa esta información para la empresa? Es decir, cuidar la información es cuidar la propia existencia de la compañía. Cada vez que se menciona la palabra Información se hace referencia a la Información que es procesada por un Sistema Informático; definiendo este último como el "conjunto formado por las personas, computadoras (hardware y software), papeles, medios de almacenamiento digital, el entorno donde actúan y sus interacciones."

La seguridad es un concepto abstracto difícil de definir, podríamos pensarla como una sensación de protección, que depende de varios factores (el contexto, nuestras fortalezas, nuestras debilidades, las amenazas). Si unimos estas definiciones, podríamos intentar una definición de seguridad de la información, diciendo que es la sensación que perciben las personas sobre el nivel de protección de la información.

La seguridad de la información se encarga de protegerla de una amplia gama de amenazas, a fin de garantizar la continuidad del negocio, minimizar los daños y maximizar el retorno sobre las inversiones y las oportunidades, normalmente se

logra implementando un conjunto adecuado de controles que abarcan políticas y procedimientos, involucrando recursos humanos, hardware y software.

El término seguridad de la información cubre un amplio espectro de actividades, y parte de nuestro trabajo como auditores informáticos con amplios conocimientos sobre seguridad, será hacer recomendaciones y tomar acciones para minimizar los riesgos y exposición de la información y demás activos. Estas actividades de control en la seguridad de la información, muchas veces no son sencillas, pero deberemos realizarlas correctamente para tener la opción de mantener la seguridad de la información de la empresa dentro de niveles razonables.

## **1.2.- NECESIDAD DE GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN**

La información y los sistemas de procesamiento, por un lado, y los sistemas de comunicaciones y las redes que le brindan apoyo son importantes recursos de toda empresa moderna.

Hoy en día son esenciales para el normal desenvolvimiento de las tareas, es decir, si una empresa no tiene información se paraliza, piense que sucede si se corta el acceso a Internet en una empresa moderna, los usuarios, especialmente los gerentes, comienzan a impacientarse, porque no pueden enviar y recibir sus correos electrónicos, o porque no pueden consultar las últimas noticias de los mercados en la WEB, esto ejemplos bastan para darnos una idea de cuan necesaria es la información.

Actualmente las empresas han ido reforzando poco a poco sus medidas de seguridad pero no saben en que momento pueden estar expuestas, conocen muy poco sobre cual es el riesgo que tienen y su nivel de impacto.

Las empresas invierten tiempo y dinero en implementar grandes infraestructuras tecnológicas que soporten todas las operaciones del negocio, pero todo este escenario tecnológico puede ser una gran debilidad cuando esta se ve comprometida.

Los riesgos son sustanciales y las tecnologías comunes tan complejas que requieren de prácticas específicas en seguridad informática para garantizar la supervivencia de la infraestructura tecnológica.

Por lo tanto es vital implementar un Plan de Gestión de Seguridad de la Información, pero este plan debe ser proactivo acorde al tamaño de la empresa y las necesidades del negocio que les indique como desenvolverse en los distintos escenarios que se le puedan presentar y prepararse de las amenazas que se podrían presentar a futuro.

Cuando hablamos de seguridad de la información generalmente nos referimos a aquellas prácticas, herramientas y metodologías destinadas a proteger los sistemas informáticos de abusos; sean estos internos o externos. Es importante recordar que las amenazas internas son igualmente importantes para la seguridad de una red o un sistema, dado que el 60-70% de los problemas de seguridad tienen origen interno.

Conceptualmente hablamos de sistemas seguros cuando estos se comportan como esperado: son confiables, distribuyen información de acuerdo a una política de acceso, permiten que la información esté disponible cuando la necesitamos, evitan que personas no autorizadas accedan a servicios y/o información, salvaguardan información confidencial, permiten la distribución de información limitada, etc.

La tendencia ahora es prepararse ante múltiples escenarios en los que de una otra forma pueda salir perjudicada la empresa.

El tener un Plan de Gestión de Seguridad de la Información le aportara un valor intrínseco al negocio, mejorará su credibilidad, aumentara confianza de accionistas principales y lo mas importante le dará una ventaja estratégica a la empresa.

Usadas correctamente, estas herramientas y metodologías reducen sustancialmente el riesgo de problemas de seguridad, pero no lo eliminan. Usadas incorrectamente, estas herramientas y metodologías dan una falsa sensación de seguridad.

### **1.3.- OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**

Mencionamos antes que la seguridad de la información se encarga de protegerla, más específicamente, podemos definir que lo logrará preservando la confidencialidad, integridad y disponibilidad de la información, como aspectos fundamentales y el control y autenticidad como aspectos secundarios. A continuación se describen estas características:

### **1.3.1.- LA INTEGRIDAD DE LA INFORMACIÓN**

Es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias.

Una falla de integridad puede estar dada por muchos factores como desperfectos de hardware, mala utilización del software que maneja la información, virus informáticos y/o modificación por personas no autorizadas que se infiltran en el sistema.

### **1.3.2.- LA DISPONIBILIDAD U OPERATIVIDAD**

Aplicado a la Información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada, con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

### **1.3.3.- LA PRIVACIDAD O CONFIDENCIALIDAD**

Aplicado a la Información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona y/o los resultados de examen realizados) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se "filtran" a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes o mejorar el producto propuesto).

El Control sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma, protegiendo su integridad.

### **1.3.4.- LA AUTENTICIDAD**

Permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Adicionalmente a los conceptos anotados pueden considerarse algunos otros aspectos, relacionados con los anteriores, pero que incorporan algunas consideraciones particulares:

#### **1.3.5.- PROTECCIÓN A LA RÉPLICA**

Mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.

#### **1.3.6.- NO REPUDIO**

Mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

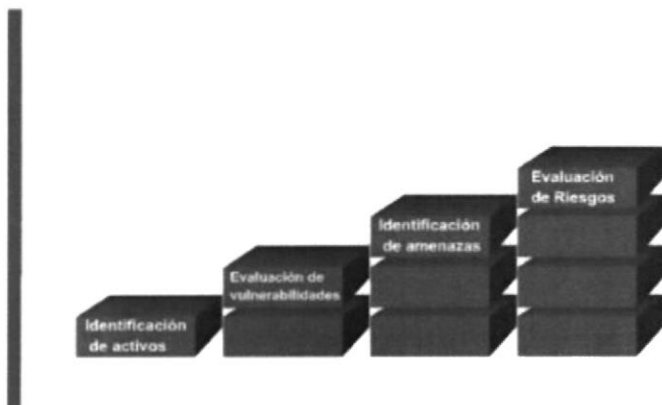
#### **1.4.- ASPECTOS GENERALES DE LA SITUACIÓN ACTUAL EN SEGURIDADES**

Es muy importante que una organización realice un examen consciente de su actual situación respecto a la seguridad, este análisis deberá incluir los aspectos mas relevantes de su actividad y los procesos que se realizan para proteger la información, así como los equipos que la procesan, esto permitirá tomar acciones en caso que el resultado indique que se encuentra en una situación comprometida. El examen implica los siguientes pasos:

- Identificación de activos
- Evaluación de vulnerabilidades
- Identificación de amenazas
- Estimación de los riesgos

Estas cuatro acciones le ayudarán a identificar cuales recursos vale la pena proteger, y a valorizarlos, debido a que algunos son más importantes que otros, además esta evaluación le ayudará a la hora de definir los recursos económicos y humanos destinados para su protección. En la figura podemos observar la relación entre las cuatro acciones.

## Relación entre los requerimientos



### 1.4.1.- ACTIVOS

Cada organización tiene activos y recursos valiosos. La identificación de activos es el proceso por medio del cual una compañía intenta evaluar la información y sus sistemas. En algunos casos, es tan simple como contabilizar las licencias de software; estas valuaciones de activos físicos son parte de un proceso de contabilización normal que una empresa debería realizar en forma rutinaria.

La parte más difícil del proceso de identificación de activos es intentar asignarle un valor o un peso cuantificable a la información. En algunos casos, podría ayudarnos si intentamos determinar que sucedería en caso que la información se pierda o se vuelva no disponible.

Si la ausencia de esta información provoca que el negocio se detenga, esta información es muy valiosa y se podrá evaluar según el costo que le provoque a la empresa esta detención.

Es importante identificar todos los recursos de la red (computadores, impresoras, bases, equipos de comunicación, etc.) que podrían verse afectados por un problema de seguridad. Podemos mencionar los siguientes ejemplos de activos asociados a sistemas de información:

### 1.4.2.- RECURSOS DE INFORMACIÓN

Bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de

continuidad, disposiciones relativas a sistemas de emergencia para la reposición de información perdida, información archivada.

#### **1.4.3.- RECURSOS DE SOFTWARE**

Software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios.

#### **1.4.4.- ACTIVOS FÍSICOS**

Equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PBXs, máquinas de fax, etc.), medios magnéticos (cintas y discos), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado), mobiliario, etc.

#### **1.4.5.- SERVICIOS**

Servicios informáticos y de comunicaciones, utilitarios generales, por ej., iluminación, energía eléctrica, aire acondicionado.

#### **1.5.- VULNERABILIDADES**

Probablemente las capacidades de seguridad del software y los sistemas utilizados en la organización es el área de mayor interés para el especialista de seguridad. A través del estudio de estas capacidades, podrá detectar las vulnerabilidades y fortalecer el sistema antes que los malintencionados se aprovechen.

Hasta hace poco tiempo, muchos desarrolladores de sistemas operativos no prestaban especial atención a las características de seguridad. Por ejemplo, un sistema operativo muy popular utiliza un esquema de seguridad que descansa en un logon y password, pero cuando aparece el mensaje de logon, en lugar de ingresar las credenciales, todo lo que tiene que hacer es un click sobre el botón Cancelar y el sistema le permitirá utilizar la mayoría de las capacidades de red y acceso local a todos los recursos. Esto es peor que no tener seguridad, porque muchos usuarios pensando en estas características supondrán que tienen un sistema seguro. Esto no es así, y como resultado ocurren muchos hurtos de información.

Los sistemas operativos y programas de aplicación han sido vulnerables a ataques internos y externos por mucho tiempo. Las compañías de software quieren vender software que sea fácil de utilizar, con interfaces gráficas, y fácilmente configurables.

Los usuarios quieren lo mismo. Desafortunadamente, esta facilidad de uso y configuración generalmente crea problemas de seguridad adicionales. Por ejemplo, uno de los productos más populares en la actualidad permite que los e-mails y attachments puedan ejecutar programas embebidos en un mensaje. Esto permite crear mensajes de e-mail con fantásticas presentaciones, pero también permite que los mensajes puedan llevar virus que pueden dañar la computadora y desparramarse hacia otras redes. El desarrollador de este software ha creado una actualización de seguridad, pero se observa que cada vez que se introduce una actualización, alguien encuentra una forma de saltarla.

#### **1.6.- AMENAZAS A LA SEGURIDAD**

Una vez identificados los recursos que necesitan protección, deberá identificar cuáles son las amenazas a estos recursos, y poder determinar qué potencial de daño o pérdida existe. Por otro lado, deberá determinar de cuáles amenazas tratará de proteger a los recursos en función de la probabilidad de ocurrencia.

La implementación de una política de seguridad requiere que no solo se evalúen las amenazas, sino también el origen, así como el impacto que tendrían en la organización si estas amenazas se vuelven realidad, de esta forma tendremos amenazas externas e internas. Por ejemplo, será poco provechoso implementar un ambiente de alta seguridad para proteger la empresa de los usuarios del exterior, si las amenazas provienen principalmente del interior.

Si un miembro de la empresa trae un diskette con un documento que contiene un virus y lo abre en la PC de la oficina, el virus podría expandirse a través de toda la red, para este caso no hubieran servido de nada las mejores medidas de seguridad externas.

Entre las amenazas más comunes podemos encontrar, daño en equipos locales o remotos, pérdida de comunicación y de información, el acceso no autorizado a la red y a los sistemas, denegación de servicio, ausencia del servicio, fraude y alteración de datos.



### **1.7.- RIESGO Y CONTROL**

Los requerimientos a cubrir en el área de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. Las erogaciones derivadas de la satisfacción de las necesidades de control deben ser equilibradas con respecto al impacto potencial de las fallas de seguridad en los negocios.

La evaluación de riesgos es una consideración sistemática de los siguientes puntos:

### **1.8.- IMPACTO**

El impacto potencial de una falla de seguridad en los negocios, teniendo en cuenta las potenciales consecuencias por una pérdida de la confidencialidad, integridad o disponibilidad de la información y otros recursos.

### **1.9.- PROBABILIDAD**

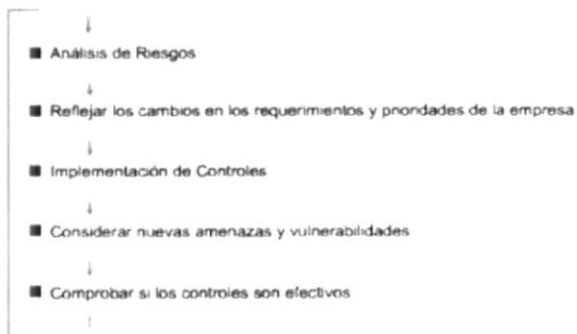
La probabilidad de ocurrencia de dicha falla se materialice tomando en cuenta las amenazas y vulnerabilidades predominantes, y los controles actualmente implementados.

Los resultados de esta evaluación ayudarán a orientar ya determinar las prioridades y acciones de gestión adecuadas para la administración de los riesgos concernientes a seguridad de la información, y para la implementación de los controles seleccionados a fin de brindar protección contra dichos riesgos y reducirlos a un nivel aceptable.

Es importante llevar a cabo revisiones periódicas de los riesgos de seguridad y de los controles implementados a fin de:

- Reflejar los cambios en los requerimientos y prioridades de la empresa;
- Considerar nuevas amenazas y vulnerabilidades;
- Corroborar que los controles siguen siendo eficaces y apropiados

## Riesgo y Control



### 1.10.- ANÁLISIS DE RIESGOS

El análisis de riesgos implica determinar lo siguiente:

- Qué necesita proteger.
- De quién debe protegerlo.

#### 1.10.1- ¿CÓMO PROTEGERLO?

Los riesgos se pueden clasificar por el nivel de importancia y por la severidad de la pérdida. Esta valoración es muy útil, porque no debería llegar a una situación donde gasta más para proteger aquello que es menos valioso o aquello donde el costo de recuperarlo es inferior al de la pérdida.

Entre los factores que tenemos que considerar para realizar una correcta evaluación del riesgo, encontramos:

El riesgo de pérdida del recurso, que dependerá de las amenazas a las que está expuesto, las contramedidas implementadas para protegerlo y sus vulnerabilidades asociadas. Es un arte que depende del conocimiento y experiencia del evaluador.

La importancia que representa el recurso para la empresa, evaluada según cada tipo, de acuerdo a los siguientes factores:

#### 1.10.2.- DISPONIBILIDAD

Es la medida de que tan importante es tener el recurso disponible todo el tiempo.

### **1.10.3.- INTEGRIDAD**

Es la medida de cuán importante es que el recurso o los datos del mismo sean consistentes. Esto es de particular trascendencia para los recursos de bases de datos.

### **1.10.4.- CONFIDENCIALIDAD**

Es la medida de cuán importante es que los recursos solo sean observados por las personas autorizadas.

### **1.11.- TIPOS DE AMENAZAS DE SEGURIDAD**

Las organizaciones, sus redes y sistemas de información enfrentan crecientes amenazas a su seguridad que incluye el fraude asistido por computadora, actos de espionaje, sabotaje, vandalismo y hasta incendios e inundaciones.

En este contexto, amenaza informática es todo aquello capaz de manifestarse en forma de ataque a la red y provocar daños en los activos, por este motivo el profesional de seguridad debe conocer cuales son las posibles amenazas que existen en la actualidad, y mantenerse actualizado sobre las nuevas amenazas que aparezcan. Este conocimiento le permitirá realizar un correcto análisis de la situación respecto a la seguridad en la que se encuentra una organización.

Podemos realizar una clasificación de las amenazas según su origen, así encontramos las siguientes categorías:

- Amenazas físicas
- Catástrofes naturales
- Fraude informático
- Error humano
- Intrusiones
- Software ilegal
- Código malicioso

Como vemos, no todas las amenazas son generadas por usuarios malintencionados, como el Fraude informático, las Intrusiones, o el Código malicioso, sino que pueden

surgir de acciones descuidadas, negligencia, fallos de planificación, como las Amenazas Físicas, Errores Humanos o instalación de Software Ilegal.

### **1.12.- OBJETIVO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI**

El principal objetivo de un Sistema de Gestión de Seguridad de la Información es hacer conocer al personal administrativo, gerentes, y demás usuarios, sus obligaciones respecto a la protección de los recursos tecnológicos e información. El Sistema basado en una política de seguridad especificaría los mecanismos a través de los cuales se debería regir para cumplir estas responsabilidades. Otra finalidad es proporcionar una referencia a partir de la cual diseñar, configurar y/o auditar sistemas de computación y redes.

La política de seguridad también permite guiar y proporcionar apoyo gerencial para lograr los objetivos que la empresa desea en cuanto a confidencialidad, integridad y disponibilidad de la información.

En consecuencia, si una organización comienza a implementar medidas de protección sin tener al menos una política de seguridad tácita o sobreentendida estaría cometiendo un grave error, porque los medios técnicos no bastan para brindar seguridad, sino que deben estar apoyados por las políticas y procedimientos correspondientes.

### **1.13.- RESPONSABILIDADES EN UN SGSI (SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN)**

Como comentamos anteriormente, un aspecto importante de un SGSI y de la política de seguridad es asegurar que todos saben cual es su responsabilidad para mantener la seguridad.

El Sistema debe garantizar que cada tipo de problema, aún aquellos desconocidos, está asociado con alguien que pueda manejarlo de manera responsable, de esta manera se evitarán incidentes o, al menos, se minimizará su impacto. Esto es muy importante, porque debemos ser conscientes que es difícil para un Sistema de seguridad de red anticipar todas las amenazas posibles.

De igual forma pueden existir varios niveles de responsabilidad asociados con una política, por ejemplo, cada usuario deberá ser responsable de guardar su contraseña. Un usuario que pone en riesgo su cuenta aumenta la probabilidad de comprometer otras cuentas y recursos. Por otro lado, los administradores de red y sistema son responsables de mantener la seguridad general.

#### **1.14.- APOYO POLÍTICO**

Para implantar con éxito un Sistema de Gestión de Seguridad el nivel gerencial debe establecer una dirección política clara, demostrar apoyo y compromiso con respecto a la seguridad de la información, es decir debe respaldar y apoyar para asegurar su cumplimiento. Una forma de demostrar este compromiso será asignar los recursos necesarios para garantizar su desarrollo y posterior mantenimiento.

Estos recursos no sólo deberán ser económicos, sino también humanos y de infraestructura, por ejemplo deberá garantizar un espacio físico y la colaboración de gerentes, usuarios, administradores, diseñadores de aplicaciones, auditores y personal de seguridad, y expertos en áreas como legislación y administración de riesgos.

Dentro del Marco Conceptual COBIT, existe un análisis que muestra la situación actual de la organización con respecto a la seguridad, evalúa aspectos plenamente identificados como procesos relacionados a seguridad, este análisis nos permite realizar una proyección de lo que podríamos realizar si se toman los correctivos necesarios ajustados a los estándares de seguridad, lo que mostrado a la gerencia de la organización nos permitirá de cierta manera conseguir el apoyo necesario para poder implementar el Sistema de Gestión de Seguridad.

#### **1.15.- ¿GASTO O INVERSIÓN?**

Históricamente asegurar los activos informáticos ha sido considerado como un gasto para muchas empresas, y fue así como varios proyectos millonarios de comunicaciones, ERP o bases de datos sufrieron posteriormente un costo por incidentes o ataques informáticos varias veces mayor al que hubiera correspondido a tomar los recaudos necesarios para minimizar los riesgos.

Se habla generalmente de este tema como un proceso de "tomar conciencia", cuando en realidad la seguridad informática, en general, y el desarrollo y

mantenimiento de la política de seguridad en particular no es ni más ni menos que otro proyecto al que hay que encontrarle la viabilidad económica para que se considere inversión y no gasto.

Luego de conseguir el apoyo político de la gerencia de la organización, necesario para el personal que busca implantar el Sistema de Gestión, contar el apoyo del personal de la organización, es por esto que se debe convencer a estos de la importancia y la sensibilidad de la información de manejar.

La pregunta siempre es ¿cuánto hay que invertir en asegurar los recursos?, es allí donde tenemos que utilizar un criterio simple que nos da la respuesta: si tenemos activos informáticos por un determinado valor, vamos a invertir más de este valor en asegurarlos?, evidentemente no. Lo importante entonces es conocer cuanto valen nuestros activos informáticos. Pero cuidado, porque tenemos valores intangibles que debemos considerar en la evaluación, piense por ejemplo, cuanto cuesta a la imagen de una compañía que ésta no pueda dar respuesta a sus clientes durante dos días porque "se cayo el sistema". Este valor dependerá de la industria en la que la empresa se desempeña, no es lo mismo un banco que una pequeña empresa textil.

Entonces, debemos tener presente que el desarrollo de un Sistema de Seguridad de la Información y su implementación es una inversión, y las consecuencias de no tomar los recaudos necesarios pueden ser muy perjudiciales para el negocio, hasta llegar a casos extremos de quiebras.

## **CAPITULO 2.- SISTEMA HOSPITALARIO DOCENTE DE LA UNIVERSIDAD DE GUAYAQUIL**

### **2.1.- ANTECEDENTES**

El Sistema Hospitalario Docente de la Universidad de Guayaquil es un escenario complejo e innovador, que ha iniciado un proceso dirigido a la excelencia asistencial, dentro del sistema de salud del Ecuador, lo que permitirá adecuar su oferta de servicios a la demanda de atención de salud, cada vez más exigente de nuestra sociedad.

Ofertando a los usuarios el mejor servicio posible, teniendo dos ejes que regirán la actividad diaria del Sistema Hospitalario que son:

- La calidad, que es el presente
- La docencia e investigación; cuyos frutos serán fundamentales para el desarrollo y fortalecimiento de la ciencia biomédica.

### **2.2.- RESEÑA HISTÓRICA**

Desde hace mucho tiempo fue motivo de iniciativas e inquietudes por parte de autoridades, profesores y alumnos de la facultad de Ciencias Médicas de la Universidad de Guayaquil, contar con un Hospital Universitario que permitiera desarrollar con mayor amplitud las actividades docentes y de investigación en el campo de la salud y es así como en el año 1967 se conforma una Comisión integrada por el Señor Decano de la Facultad de ciencias Médicas doctor Carlos Zunino Guzmán toda la comisión en representación de la Facultad de Ciencias Médicas plantean ante el H. Concejo Provincial del Guayas, presidido en ese entonces por el señor Bolívar San Lucas.

La necesidad de que la Universidad de Guayaquil tenga su hospital Universitario; planteamiento que demandó la ayuda económica por parte de ese organismo.

Como resultado, el H. Consejo Provincial del Guayas en sesión del 14 de diciembre de 1967, aprueba la creación de la partida presupuestaria N° 36557 a favor de la Universidad de Guayaquil, por el valor de dos millones de sucres anuales por un lapso de diez años a partir de 1968, hasta completar la suma de veinte millones de sucres que servirá para la construcción del hospital. Para el efecto dos años más

tarde el 24 de enero de 1969, se suscribe el respectivo Convenio ante el Notario del Cantón.

En julio de 1980 se celebra el Convenio entre los Ministerios de Educación y Cultura, salud Pública y la Universidad de Guayaquil, para proceder a la construcción, equipamiento y funcionamiento del Hospital Universitario.

### **2.3.- SHDUG ATENCION AL PUBLICO**

EL Sistema Hospitalario Docente de la Universidad de Guayaquil se inaugura el 18 de abril del 2005.

Actualmente se encuentra funcionando el edificio de maternidad; dentro del cual se brinda servicios de consulta externa, laboratorio clínico, imágenes y rayos X, inmunizaciones, terapias y procedimientos de enfermería, además de contar con una farmacia de medicamentos genéricos, además en el edificio contiguo (destinado a Docencia e Investigación) se encuentra funcionando el área de Odontología.

Para asegurar la excelencia en la prestación de sus servicios, el Sistema Hospitalario Docente de la Universidad de Guayaquil desarrollará políticas, planes, programas y eventos en el marco de procesos de gestión en todas sus áreas:

#### **2.3.1.- DOCENCIA E INVESTIGACIÓN:**

- Proyectos de aulas virtuales
- Clases en línea
- Telemedicina

#### **2.3.2.- GINECO – OBSTETRICA - PERINATOLÓGICA:**

- Hospitalización: Gineco-Obstetricia y Neonatología.
- Ambulatorio: Urgencia y consulta externa.

#### **2.3.3.- HOSPITAL DE ESPECIALIDADES:**

- Hospitalización:
  - Medicina interna



- Pediatría
- Cirugía
- Unidades de:
  - Quemados
  - Diálisis
  - Trasplantes
  - Trauma.
- Servicios ambulatorios. Urgencias de adultos, Pediátricas, Consulta Externa y Rehabilitación.
- Servicios quirúrgicos.
- Hospital del Día
- Servicio de Diagnóstico y Tratamiento.
- Unidad Odontológica
- Dispensarios periféricos
- Residencia hospitalaria.

#### **2.4.- VISION**

Será una institución de cuarto nivel de atención integral de salud, docencia en servicio, educación continua e investigación científica permanente en las ciencias de la salud; constituirá un modelo de sistema de salud nacional e internacional.

El Sistema Hospitalario Docente de la Universidad de Guayaquil en su total funcionamiento contribuirá a mejorar las condiciones de salud y vida de los ecuatorianos y fortalecerá el desarrollo académico de la Universidad de Guayaquil.

#### **2.5.- MISION**

El Sistema Hospitalario Docente de la Universidad de Guayaquil ofertará servicios de atención integral de salud a la comunidad universitaria, a sus familias y a la población del área geográfica correspondiente, con calidez, calidad técnica, científica, humana y competitiva, bajo principios de efectividad, equidad y solidaridad; fortalecerá el desarrollo del talento humano y la investigación científica.

#### **2.6.- OBJETIVOS**

- Implantar programas de atención integral de salud intra y extra institucional con recursos humanos altamente calificados con tecnología de punta y

mediante estrategias de participación social, para lograr el mejoramiento de la calidad de salud y vida de los usuarios que acuden al Sistema.

- Facilitar las actividades de docencia e investigación y extensión para la formación profesional y de postgrado que realizan las unidades académicas de la Universidad de Guayaquil.
- Desarrollar un modelo de gerencia estratégica y calidad en gestión de salud, con integración de acciones clínicas, quirúrgicas, asistenciales, docentes y de investigación técnico-científica mediante una cultura organizacional orientada a satisfacer las necesidades del usuario.
- Implantar un modelo de gestión económico - administrativo en el Sistema Hospitalario, mediante procesos y estructuras que sirvan de ejemplo para el desarrollo de otros proyectos, mediante el uso de tecnología de punta para lograr reducir costos y aumentar la eficiencia en sus procesos.
- Organizar y administrar las unidades componentes del Sistema Hospitalario Docente de la Universidad de Guayaquil.
- Promover alianzas estratégicas con instituciones del sector público, privado y organizaciones no gubernamentales, nacionales e internacionales, a fin de fortalecer el desarrollo institucional.
- Implementar una base informática que permita mantener un sistema administrativo ágil que responda a la dinámica del Sistema Hospitalario Docente, que provea de información ágil y oportuna a las necesidades tanto medicas como docentes y en el campo de la investigación científica.

## **CAPITULO 3.- COBIT**

### **3.1.- MARCO CONCEPTUAL DE DESARROLLO (ENTORNO DE TRABAJO BASADO EN PROCESOS DE COBIT)**

Las organizaciones reconocen cada vez más la importancia que reviste la Tecnología de la Información para sus organizaciones, al punto de considerarla uno de sus recursos más valiosos ya que en muchos casos representa una ventaja competitiva respecto de otras organizaciones.

Los sistemas de información ya no sólo satisfacen las necesidades internas sino que también soportan las relaciones con clientes y proveedores. Es por todo esto que se vuelve imperioso que las organizaciones también comprendan, además de los beneficios, también existen los riesgos que involucra el uso e implementación de nuevas tecnologías.

Resulta incuestionable que la revolución tecnológica que experimenta la humanidad en todas las áreas, ha demandado la generación de nuevos productos y servicios, que garanticen que la nueva tecnología incorporada a las empresas, genere valores agregados significativos en su contribución a la productividad, competitividad y eficiencia integral de la organización.

Situaciones como el aumento en la vulnerabilidad de los sistemas, altos costos de inversión en complejos sistemas de información, etc. ponen en evidencia la necesidad de un Marco de Referencia para la seguridad y el control de Tecnología de Información.

### **3.2.- ¿POR QUE COBIT?**

- El marco de trabajo del programa ha sido estructurado en 34 procesos agrupados en actividades interrelacionadas con el ciclo de vida. El modelo del proceso se prefirió por varias razones. Antes que nada, un proceso por su naturaleza está orientado al resultado; por que se focaliza en la obtención del resultado final mientras optimiza el uso de recursos. La manera que estos recursos se estructuran físicamente (gente, skills en departamentos) es menos relevante en esta perspectiva, ya que toma como factor primordial a el proceso.

- En segundo lugar, un proceso, especialmente sus objetivos, son más permanentes y el riesgo de cambio no es tan alto y frecuente como la estructura organizacional. En tercer lugar, el despliegue de IT, no puede ser limitado a un departamento en particular e involucrar a usuarios, a la administración así como especialistas de IT.
- En este contexto, los procesos de IT permanecen sin cambios como común denominador.
- A lo que las aplicaciones refiere, éstas son tratadas dentro de Cobit como uno de las cinco categorías de recurso. De ahí, que las aplicaciones deberán ser manejados y controlados de tal manera que puedan producir la información requerida en el nivel del proceso del negocio.
- De esta manera, los sistemas de aplicación son una parte esencial de Cobit y pueden ser administrados específicamente a través de los recursos. Es decir, enfocándonos estrictamente en los recursos, obtendríamos automáticamente la visión de aplicaciones de los objetivos de Cobit.
- En este contexto COBIT (metodología orientada al entendimiento y a la administración de riesgos asociados con tecnología de información) tiene como misión fundamental convertirse en una guía de buenas prácticas que permitan optimizar la inversión que la organización realiza en tecnología informática, y a su vez que dicha guía sirva también para medir cuándo las cosas no funcionan adecuadamente y cual es el mecanismo que debemos llevar acabo para corregir y atacar las causas.

### **3.3.- ¿PORQUE COBIT Y NO ISO 17799?**

- Cobit se basa en 41 estándares y en los mejores documentos de mejores prácticas para la informática, establecidos por los estándares (públicos y privados) a nivel mundial.
- Esto incluye documentos de Europa, Canadá, Australia, Japón y los Estados Unidos. Porque el Cobit contiene todos los estándares mundiales pertinentes identificables.

- Como resultado, el Cobit se puede utilizar como un documento autoritario de referencia documentada, como una fuente que proporciona la criterios de control de IT y auditorias de IT

### 3.4.- USUARIOS DE COBIT

Los destinatarios de COBIT son tres grupos bien definidos:

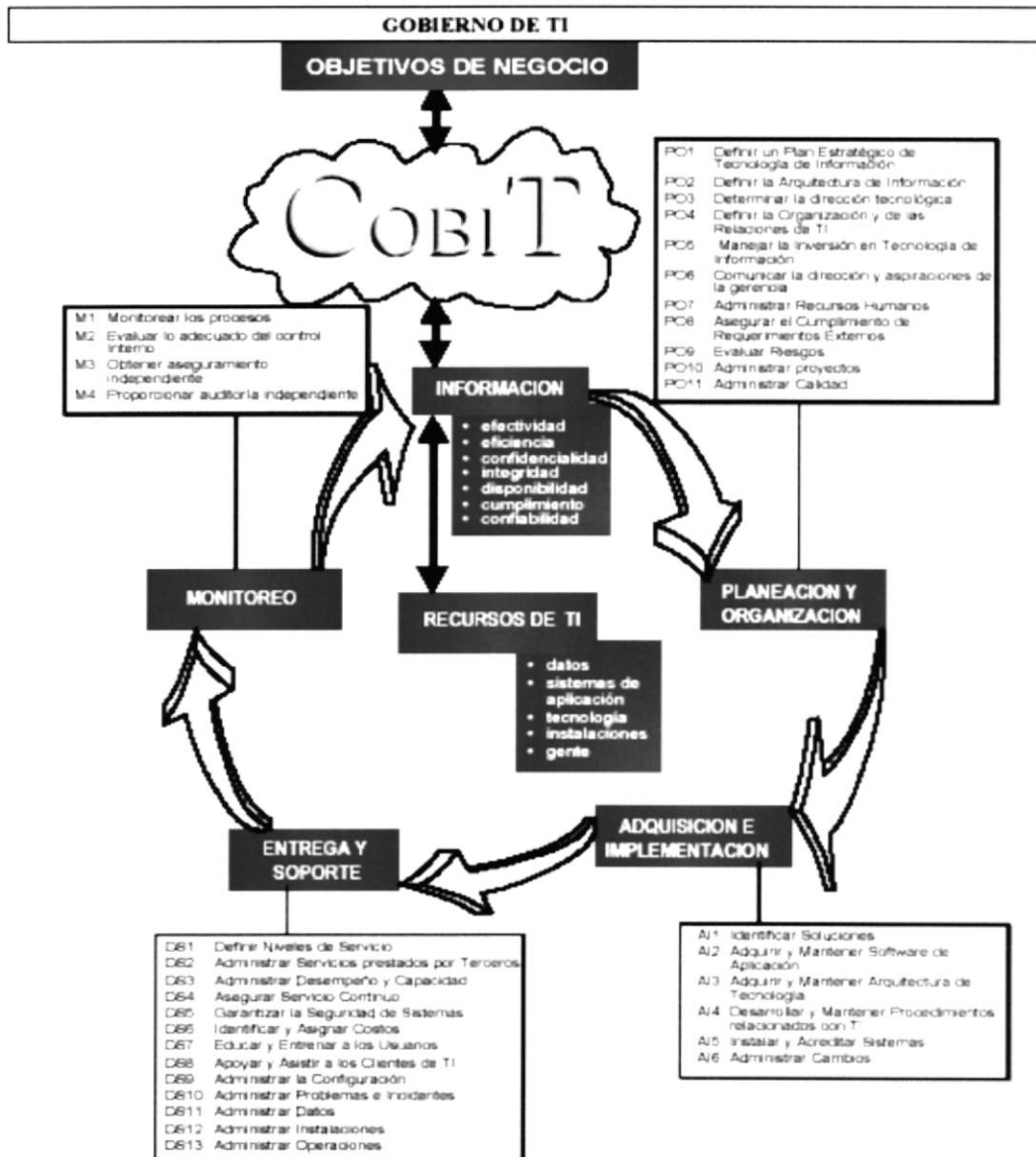
- **Gerentes:** Para ayudarlos a equilibrar el riesgo y la inversión en controles de un ambiente de TI a menudo imprevisible.
- **Usuarios:** Para obtener la garantía de la seguridad y los controles de los servicios de TI provistos por personal de la organización o terceros.
- **Audidores de Sistemas:** para respaldar sus opiniones y/o aconsejar a la gerencia con respecto a los controles internos.

La estructura de COBIT propone un marco de acción que parte de la idea que para lograr los objetivos del negocio se deben evaluar los Requerimientos del Negocio, los Recursos de TI y a los procesos de TI; los cuales pueden ser enfocados desde tres puntos ventajosos como lo son los criterios de información, como por ejemplo la seguridad y calidad, se evalúan los recursos que comprenden la tecnología de información, como por ejemplo recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

COBIT es un marco referencial y está considerado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información.

Cobit se basa en un conjunto de 34 objetivos de control de alto nivel, uno para cada uno de los procesos de tecnología de información agrupado en 4 dominios. Estos dominios se identifican con las actividades diarias de administración de TI de la organización, siendo estos:

El modelo COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas)



### 3.5.- DESCRIPCION DE DOMINIOS DE COBIT

DOMINIO	DESCRIPCION
Planificación y Organización	Este dominio abarca la estrategia y la táctica y se vincula con la identificación de la forma en que la tecnología de información puede contribuir más adecuadamente con el logro de los objetivos del Negocio. Además, es preciso planificar, comunicar y administrar la realización de la visión estratégica desde distintas perspectivas. Por último, debe existir una correcta organización e infraestructura tecnológica.
Adquisición e Implementación	Para realizar la estrategia de TI, deben identificarse, desarrollarse o adquirirse soluciones de TI y luego implementarse e integrarse en el proceso de negocio. Además, este dominio abarca los cambios y el mantenimiento de los sistemas existentes para garantizar que el ciclo de vida perdure para estos sistemas.
Entrega y Soporte	Este dominio comprende la entrega o prestación efectiva de los servicios requeridos, y abarca desde las operaciones tradicionales sobre aspectos de seguridad y continuidad hasta la capacitación. Para prestar los servicios, deben establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento real de los datos por los sistemas de aplicación, a menudo clasificados como controles de aplicaciones.
Monitoreo	Es preciso evaluar regularmente todos los procesos de TI a medida que transcurre el tiempo para determinar su calidad y el cumplimiento de los requerimientos de control. Es así que este dominio corresponde a la vigilancia de la gerencia sobre los procesos de control de la organización y a la garantía independiente provista por la auditoria interna y externa u obtenida de fuentes alternativas.

Este esquema de dominios permite una fácil navegación del producto ya que permite acceder a la información desde un nivel general DOMINIO hasta un nivel de detalle menor, que es la actividad. En el siguiente cuadro se muestra cómo Cobit

propone el acceso a la información para los distintos dominios, en este caso se observa el dominio Planeamiento y Organización.

### 3.6.- MARCO REFERENCIAL



DOMINIO	PROCESO	Criterios de Información						Recursos de TI						
		E	E	C	I	A	C	R	P	A	T	F	D	
Planeamiento y Organización	P01 Definir un plan estratégico de sistemas	P	S						X	X	X	X	X	
	P02 Definir la arquitectura de información	P	S	S	S					X			X	
	P03 Determinar la dirección tecnológica	P	S								X	X		
	P04 Definir la organización y sus relaciones	P	S						X					
	P05 Administrar las inversiones (en TI)	P	P					S	X	X	X	X		
	P06 Comunicar la dirección y objetivos de la gerencia	P						S	X					
	P07 Administrar los recursos humanos	P	P						X					
	P08 Asegurar el apego a disposiciones extremas	P						P	S	X	X			X
	P09 Evaluar riesgos	P	S	P	P	P	S	S	X	X	X	X	X	
	P010 Administrar proyectos	P	P						X	X				
	P011 Administrar calidad	P	P		P			S	X	X				

Referencias	Criterios de Información		Recursos de Información	
	E	EFFECTIVIDAD	P	RECURSOS HUMANOS
	E	EFICIENCIA	A	SISTEMAS DE INFORMACIÓN
	C	CONFIDENCIALIDAD	T	TECNOLOGÍA
	I	INTEGRIDAD	F	INSTALACIONES
	A	DISPONIBILIDAD	D	DATOS
	C	CUMPLIMIENTO		
	R	CONFIABILIDAD		

P= Primario  
S= Secundario

**Primario.-** Es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.

**Secundario.-** Es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.



**Blanco (vacío).** - Podría aplicarse o no, sin embargo los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

En la tabla resumen podemos observar los distintos procesos vinculados al dominio denominado Planeamiento y Organización. Así por ejemplo podemos observar que para el proceso 01 denominado "Definir un plan estratégico de sistemas", los criterios de información requeridos son Efectividad como criterio primario y Eficiencia como criterio secundario y los recursos de tecnología de información involucrados son todos (Recursos Humanos, Sistemas de Información, Tecnología, Instalaciones y Datos).

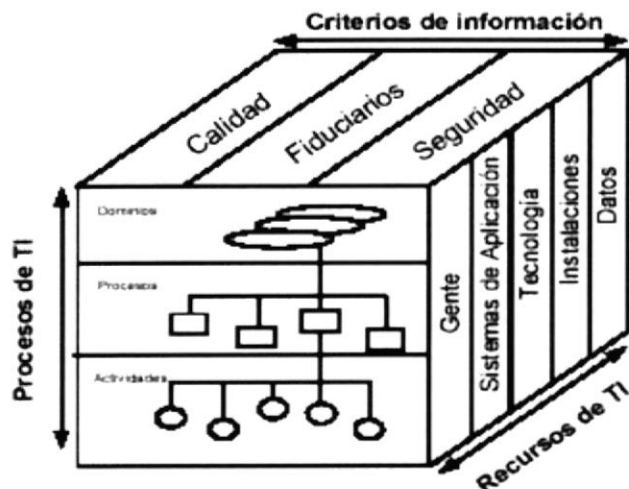
De esta forma podemos ver rápidamente cuáles son los requerimientos del negocio y los recursos involucrados en el mismo. Luego, a nivel de cada proceso se indican las pautas observadas para cada uno de ellos, los objetivos de control a ser cubiertos, qué aspectos deben analizarse, qué debe evaluarse de los controles, qué elementos deben verificarse y cómo debe tratarse el respectivo riesgo.

De esta forma se puede ir de lo general a lo particular para cada uno de los dominios de acuerdo a la necesidad de profundizar el análisis que exista.

Esta tabla solo toma un dominio de los cuatro que posee Cobit para una comprensión integral de cómo se definió nuestro entorno de trabajo y cual fue el análisis realizado, el gráfico completo con los 4 dominios y los objetivos de control se encuentra en el Anexo A adjunto.

La estructura conceptual se puede enfocar desde tres puntos de vista:

- Los recursos de las TI,
- Los criterios empresariales que debe satisfacer la información, y
- Los procesos de las TI.



De esta misma forma nos basamos en los 3 requerimientos de Seguridad que son: Confidencialidad, Integridad y Disponibilidad y en nuestra matriz ubicaremos estos criterios de información y cuales son los procesos que están relacionados de forma primaria.

Los procesos relacionados con la seguridad de la información que fueron identificados son:

- Evaluación de Riesgos.
- Administración de Calidad
- Administrar Cambios
- Aseguramiento de Servicio Continuo
- Garantizar la seguridad de Sistemas
- Administrar la información
- Administrar las Instalaciones

Luego detallaremos todos los controles correspondientes a cada uno de los objetivos de control, de los cuales se obtuvieron 101 actividades de control. Una vez obtenido esto efectuamos una auto evaluación de los procesos de seguridad de tecnología de información basados en el modelo de madurez

### 3.7.- MODELO DE MADUREZ PARA AUTOEVALUACION

Es un método de medición para determinar "que tan avanzado" está un proceso en cuanto a su control, respecto de un ideal.

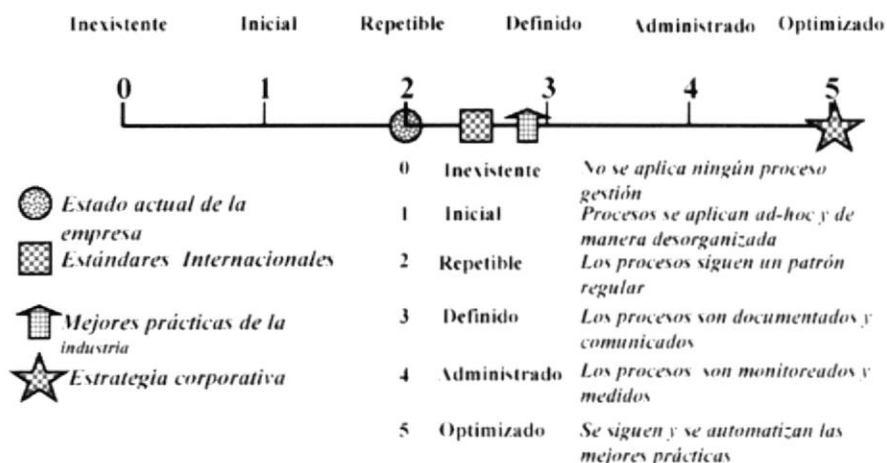
Permite identificar debilidades, prioridades de mejoramiento y mejora el conocimiento global de cómo esta la empresa así como desarrollar estrategias específicas por cada proceso

### 3.8.- NIVELES DE MADUREZ DE LA ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD

Nivel	Estado	Definición
0	No existe	La directiva (o el proceso) no está documentada y la organización, anteriormente, no ha tomado conciencia del riesgo de negocios asociado a esta administración de riesgos. Por lo tanto, no ha habido comunicados al respecto.
1	Ad hoc	Es evidente que algunos miembros de la organización han llegado a la conclusión de que la administración de riesgos tiene valor. No obstante, los esfuerzos de administración de riesgos se han llevado a cabo de un modo ad hoc. No hay directivas o procesos documentados y el proceso no se puede repetir por completo. En general, los proyectos de administración de riesgos parecen caóticos y sin coordinación; los resultados no se han medido ni auditado.
2	Repetible	Hay una toma de conciencia de la administración de riesgos en la organización. El proceso de administración de riesgos es repetible aunque inmaduro. El proceso no está totalmente documentado; no obstante, las actividades se realizan periódicamente y la organización está trabajando en establecer un proceso de administración de riesgos exhaustivo con la participación de los directivos. No hay cursos formales ni comunicados acerca de la administración de riesgos; la responsabilidad de la implementación está en manos de empleados individuales.

Nivel	Estado	Definición
3	Proceso definido	<p>La organización ha tomado una decisión formal de adoptar la administración de riesgos incondicionalmente con el fin de llevar a cabo su programa de seguridad de información. Se ha desarrollado un proceso de línea de base en el que se han definido los objetivos de forma clara con procesos documentados para lograr y medir el éxito. Además, todo el personal dispone de algunos cursos de administración de riesgos rudimentaria. Finalmente, la organización está implementando de forma activa sus procesos de administración de riesgos documentados.</p>
4	Administrado	<p>Hay un conocimiento extendido de la administración de riesgos en todos los niveles de la organización. Los procedimientos de administración de riesgos existen, el proceso está bien definido, la comunicación de la toma de conciencia es muy amplia, hay disponibles cursos rigurosos y se han implementado algunas formas iniciales de medición para determinar la efectividad. Se han dedicado recursos suficientes al programa de administración de riesgos, muchas partes de la organización disfrutan de sus ventajas y el equipo de administración de riesgos de seguridad puede mejorar continuamente sus procesos y herramientas. Se utilizan herramientas de tecnología como ayuda para la administración de riesgos, pero la mayoría de los procedimientos, si no todos, de evaluación de riesgos, identificación de controles y análisis de costo-beneficios son manuales.</p>
5	Optimizado	<p>La organización ha dedicado recursos importantes a la administración de riesgos de seguridad y los miembros del personal miran al futuro intentando determinar los problemas y soluciones que habrá en los meses y años venideros. El proceso de administración de riesgos se ha comprendido bien y se ha automatizado considerablemente mediante el uso de herramientas (desarrolladas internamente o adquiridas a proveedores de software independientes). La causa principal de todos los problemas de seguridad se ha identificado y se han adoptado medidas adecuadas para minimizar el riesgo de repetición. El personal dispone de cursos en distintos niveles de experiencia.</p>

### 3.9.- REPRESENTACION GRAFICA DEL MODELO DE MADUREZ



### 3.10.- EVALUACION DE RIESGOS

#### 3.10.1.- VALORACIÓN DEL RIESGO

La valoración del riesgo consta de tres etapas: La identificación, el análisis y la determinación del nivel del riesgo. Para cada una de ellas es necesario tener en cuenta la mayor cantidad de datos disponibles y contar con la participación de las personas que ejecutan los procesos y procedimientos para lograr que las acciones determinadas alcancen los niveles de efectividad esperados.

Para esto se utilizaron diferentes fuentes de información del Sistema Hospitalario Docente de la Universidad de Guayaquil, tales como registros históricos y experiencias significativas registradas sobre el tema.

#### 3.10.2.- IDENTIFICACIÓN DEL RIESGO

El proceso de la identificación del riesgo debe ser permanente e interactivo, integrado al proceso de planeación y responder a las preguntas qué, como y por qué se pueden originar hechos que influyen en la obtención de resultados.

Una manera de realizar la identificación del riesgo es a través de la elaboración de un mapa de riesgos con los objetivos de control de Cobit que fueron identificados,

definiendo en primera instancia los riesgos, posteriormente presentando una descripción de cada uno de ellos y las posibles consecuencias.

### **3.10.3.- ANÁLISIS DEL RIESGO**

Su objetivo es establecer una valoración y priorización de los riesgos con base en la información ofrecida por los mapas elaborados en la etapa de identificación, con el fin de clasificar los riesgos y proveer información para establecer el nivel de riesgo y las acciones que se van a implementar.

Se han establecido dos aspectos para realizar el análisis de los riesgos identificados:

### **3.10.4.- PROBABILIDAD**

La posibilidad de ocurrencia del riesgo, la cual puede ser medida con criterios de frecuencia o teniendo en cuenta la presencia de factores internos y externos que puedan propiciar el riesgo, aunque éste no se haya presentado nunca.

Para el análisis cualitativo se estableció una escala de medida cualitativa en donde se establecen unas categorías a utilizar y la descripción de cada una de ellas, con el fin que cada persona la aplique, por ejemplo:

- ALTA: Es muy factible que el hecho se presente
- MEDIA: Es factible que el hecho se presente
- BAJA: Es poco factible que el hecho se presente

### **3.10.5.- IMPACTO**

Consecuencias o impacto que puede ocasionar a la organización la materialización del riesgo en aspectos como imagen, impacto económico, reputación, entre otros.

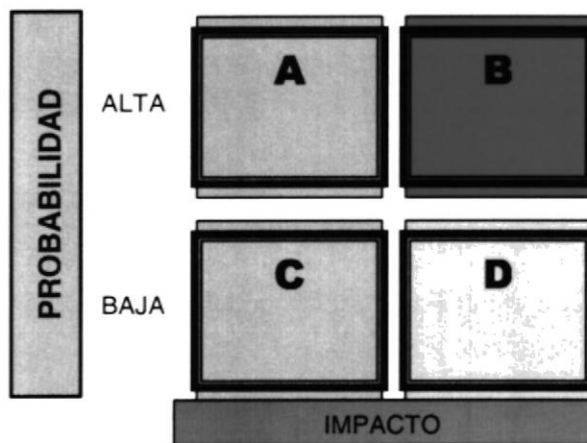
Ese mismo diseño puede aplicarse para la escala de medida cualitativa de Impacto, estableciendo las categorías y la descripción, por ejemplo:

- ALTO: Si el hecho llegara a presentarse, tendría alto impacto o efecto sobre la Entidad.
- MEDIO: Si el hecho llegara a presentarse tendría medio impacto o efecto en la entidad.

- **BAJO:** Si el hecho llegara a presentarse tendría bajo impacto o efecto en la entidad.

### 3.10.6.- PRIORIZACIÓN DE LOS RIESGOS

Una vez realizado el análisis de los riesgos con base en los aspectos de probabilidad e impacto, luego se utiliza la matriz de priorización que permite determinar cuales riesgos requieren de un tratamiento inmediato.



Cuando se ubican los riesgos en la matriz se define cuales de ellos requieren acciones inmediatas, que en este caso son los del cuadrante B, es decir los de alto impacto y alta probabilidad, respecto a los riesgos que queden ubicados en el cuadrante A y D, se debe seleccionar de acuerdo a la naturaleza del riesgo, ya que estos pueden ser peligrosos para el alcance de los objetivos institucionales por las consecuencias que presentan los ubicados en el cuadrante D o por la constante de su presencia en el caso del cuadrante A.

### 3.10.7.- DETERMINACIÓN DEL NIVEL DEL RIESGO

La determinación del nivel de riesgo es el resultado de confrontar el impacto y la probabilidad con los controles existentes al interior de los diferentes procesos y procedimientos que se realizan. Se deben tener muy claros los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones, estos niveles de riesgo pueden ser:

- **ALTO**: Cuando el riesgo hace altamente vulnerable a la entidad o dependencia. (Impacto y probabilidad alta versus controles existentes)
- **MEDIO**: Cuando el riesgo presenta una vulnerabilidad media. (Impacto alto - probabilidad baja o Impacto bajo - probabilidad alta versus controles existentes).
- **BAJO**: Cuando el riesgo presenta vulnerabilidad baja.( Impacto y probabilidad baja versus controles existentes).

Lo anterior significa que a pesar que la probabilidad y el impacto son altos confrontado con los controles se puede afirmar que el nivel de riesgo es medio y por lo tanto las acciones que se implementen entraran a reforzar los controles existentes y a valorar la efectividad de los mismos.

En base a este análisis de riesgo e impacto que se ha seguido tenemos como resultado el siguiente cuadro con su respectiva valoración del riesgo.



## **CAPITULO 4.- METODOLOGIA DE DESARROLLO DEL TRABAJO**

### **4.1.- SELECCIÓN DE OBJETIVOS DE CONTROL**

Como primer paso debemos seleccionar los objetivos de control relacionados con seguridad, estos objetivos fueron seleccionados de acuerdo a tres criterios relacionados con la seguridad de la información como son: seguridad, confidencialidad e integridad, como resultado de esta primera selección obtuvimos 101 objetivos de control, relacionados con 7 procesos.

### **4.2.- NIVEL DE MADUREZ (SIETE PROCESOS)**

Este nivel de madurez se aplica a los 7 procesos para conocer en que nivel se encuentra la Institución lo cual nos dio como resultado lo siguiente:

<b>Procesos</b>	<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>Nivel Esperado</b>
Evaluación de Riesgos.	*						3
Administración de Calidad	*						3
Administrar Cambios		*					3
Aseguramiento de Servicio Continuo		*					3
Garantizar la seguridad de Sistemas		*					3
Administrar la información		*					3
Administrar las Instalaciones		*					3

### **4.3.- OBJETIVOS PRIMARIOS PARA SISTEMA HOSPITALARIO - PRIORIZACION**

Luego del análisis de la situación actual se realizó una selección de los objetivos de control más importantes para el Sistema Hospitalario, además se priorizó el orden en que van a ser atendidos los procesos, el resultado de esta selección realizada con personal del Departamento de Informática arrojó 40 objetivos de control distribuidos en los 7 procesos detallados con anterioridad y que se detallan a continuación:

Procesos	Objetivos	Prioridad
Evaluación de Riesgos	3	7
Administrar Calidad	9	4
Administrar Cambios	2	3
Asegurar continuidad de Servicio	3	5
Garantizar la seguridad de Sistemas	11	2
Administrar la información	9	1
Administrar las instalaciones	3	6

#### **4.4.- CONCLUSIONES DE PRIORIZACION**

Luego de seleccionar los siete procesos claves que debe tener una organización para garantizar la seguridad de la información, podemos concluir que los directivos tienen conciencia que el proceso de evaluación y administración de riesgos es un proceso clave, pero por la forma como empezó el funcionamiento de la organización, los esfuerzos de administración de riesgos se han llevado a cabo de un modo ad hoc, no hay directivas o procesos documentados y el proceso básico de administración en la mayoría de las veces no se puede llevar a cabo por completo. En general, los proyectos de administración de riesgos de seguridad aparece sin coordinación; los resultados no se han medido ni auditado, aunque en los últimos meses se han realizado esfuerzos para documentar ciertos procesos relacionados con el desarrollo de sistemas.

Los directivos de la organización luego de una evaluación haciendo conciencia de la importancia de la evaluación de riesgos de seguridad han propuesto llegar a un nivel 3 donde se ha tomado una decisión formal de adoptar la administración de riesgos incondicionalmente con el fin de llevar a cabo su programa de seguridad de información, desarrollando un proceso de línea de base donde se definirán los objetivos de forma clara con procesos documentados para lograr medir el éxito.

#### **4.5.- ANALISIS DE RIESGO**

Los 40 objetivos de control seleccionados fueron sometidos a un análisis de riesgo, evaluando dos aspectos importantes como son la probabilidad de ocurrencia y el nivel de impacto en la organización, se realizó una ponderación de estos criterios, el resultado de esta evaluación son 12 criterios sobre los cuales se realizará una evaluación de los controles existentes, tanto en su diseño, como en su efectividad, el resumen de la selección se muestra en la tabla a continuación:

**4.5.1.- DETERMINACION DEL NIVEL DE RIESGO**

Proceso	Objetivo de Control	Probabilidad	Impacto	Puntaje	Selección
<b>Evaluar Riesgos</b>					
Evaluación de riesgos	La Gerencia deberá establecer un marco de referencia de evaluación sistemática de riesgos. Este marco de referencia deberá incorporar una evaluación regular de los riesgos de información relevantes para el logro de los objetivos del negocio, formando una base para determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable. El proceso deberá proporcionar evaluaciones de riesgos tanto a un nivel global como a niveles específicos del sistema (para nuevos proyectos y para casos recurrentes) y deberá asegurar actualizaciones regulares a la información sobre evaluación de riesgos utilizando los resultados de auditorias, inspecciones e incidentes identificados.	4	2	8	

<p>Identificación de Riesgos</p>	<p>La evaluación de riesgos deberá enfocarse al examen y evaluación de los elementos esenciales de riesgo, tales como activos, amenazas, elementos vulnerables, protecciones, consecuencias y probabilidad de amenaza.</p>	<p>4</p>	<p>3</p>	<p>12</p>	<p>*****</p>
<p>Aceptación de Riesgos</p>	<p>El enfoque de la evaluación de riesgos deberá asegurar la aceptación formal del riesgo residual, dependiendo de la identificación y la medición del riesgo existente, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de qué tan económico resulte implementar protecciones y controles. El riesgo residual deberá compensarse con una cobertura de seguro adecuada.</p>	<p>5</p>	<p>2</p>	<p>10</p>	
<p><b>Administrar Calidad</b></p>					
<p>Planeación del Aseguramiento de la Calidad</p>	<p>La Gerencia deberá implementar un proceso de planeación de aseguramiento de calidad para determinar el alcance y la duración de las actividades de</p>	<p>4</p>	<p>2</p>	<p>8</p>	

	aseguramiento de calidad.				
Revisión del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares y Procedimientos de la Función de Servicios de Información	La Gerencia deberá asegurar que las responsabilidades asignadas al personal de aseguramiento de calidad incluyan una revisión del cumplimiento general de los estándares y procedimientos de la función de servicios de información.	3	3	9	
Metodología del ciclo de vida de desarrollo de los sistemas	La alta gerencia de la organización deberá definir e implementar estándares de sistemas de información y adoptar una metodología del ciclo de vida de desarrollo de sistemas que rijan el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información computarizados y tecnología afín. La metodología del ciclo de vida de desarrollo de sistemas elegida deberá ser la apropiada para los sistemas a ser desarrollados, adquiridos, implementados y mantenidos.	3	3	9	

<p>Metodología del Ciclo de Vida de Desarrollo de Sistemas para Cambios Mayores a la Tecnología Actual</p>	<p>En el caso de requerirse cambios mayores a la tecnología actual, la Gerencia deberá asegurar el cumplimiento de la metodología del ciclo de vida de desarrollo de sistemas, como en el caso de adquisición de nueva tecnología.</p>	<p>3</p>	<p>3</p>	<p>9</p>	
<p>Actualización de la Metodología del Ciclo de Vida de Desarrollo de Sistemas</p>	<p>La alta gerencia deberá implementar una revisión periódica de su metodología del ciclo de vida de desarrollo de sistemas para asegurar que incluya técnicas y procedimientos actuales generalmente aceptados.</p>	<p>5</p>	<p>2</p>	<p>10</p>	
<p>Estándares para la Documentación de Programas</p>	<p>La metodología del ciclo de vida de desarrollo de sistemas deberá incorporar estándares para la documentación de programas que hayan sido impuestos y comunicados al personal interesado.                  La metodología deberá asegurar que la documentación creada durante el desarrollo del sistema de información sea de los proyectos nuevos o de modificación coincida con estos estándares establecidos en el marco conceptual.</p>	<p>4</p>	<p>2</p>	<p>8</p>	

<p>Estándares para Pruebas de Programas</p>	<p>La metodología del ciclo de vida de desarrollo de sistemas de la organización debe proporcionar estándares que cubran los requerimientos de pruebas, verificación, documentación y retención para probar las unidades de software y los programas agregados, creados como parte de cada proyecto de desarrollo nuevo o modificación de sistemas de información existentes.</p>	<p>5</p>	<p>2</p>	<p>10</p>	
<p>Estándares para Pruebas de Sistemas</p>	<p>La metodología del ciclo de vida de desarrollo de sistemas de la organización debe proporcionar estándares que cubran los requerimientos de pruebas, verificación, documentación y retención para probar el sistema total.                      Como parte de cada proyecto de desarrollo o modificación de sistemas de información.</p>	<p>5</p>	<p>2</p>	<p>10</p>	
<p>Documentación de las Pruebas del Sistema</p>	<p>La metodología del ciclo de vida de desarrollo de sistemas de la organización debe disponer, como parte importante de cualquier proyecto de desarrollo, implementación o modificación de sistemas</p>	<p>5</p>	<p>2</p>	<p>10</p>	

	de información, que se conserve la documentación de los resultados de las pruebas del sistema.				
<b>Administrar Cambios</b>					
Evaluación del Impacto	Deberá establecerse un procedimiento para asegurar que todas las requisiciones de cambio sean evaluadas en una forma estructurada en cuanto a todos los posibles impactos sobre el sistema operacional y su funcionalidad.	3	3	9	
Documentación y Procedimientos	El procedimiento de cambios deberá asegurar que, siempre que se implementen modificaciones a un sistema, la documentación y procedimientos relacionados sean actualizados de manera correspondiente.	3	3	9	
<b>Asegurar continuidad de Servicio</b>					



<p>Estrategia y Filosofía de Continuidad de Tecnología de Información</p>	<p>La Gerencia deberá garantizar que el Plan de continuidad de tecnología de información se encuentra en línea con el plan general de continuidad de la empresa para asegurar consistencia. Aún más, el plan de continuidad de TI debe tomar en consideración el plan a mediano y largo plazo de tecnología de información, con el fin de asegurar consistencia.</p>	<p>4</p>	<p>2</p>	<p>8</p>	
<p>Distribución del Plan de Continuidad de Tecnología de Información</p>	<p>Debido a la naturaleza sensitiva de la información del plan de continuidad, dicha información deberá ser distribuida solo a personal autorizado y mantenerse bajo adecuadas medidas de seguridad para evitar su divulgación. Consecuentemente, algunas secciones del plan deberán ser distribuidas solo a las personas cuyas actividades hagan necesario conocer dicha información.</p>	<p>4</p>	<p>2</p>	<p>8</p>	

<p>Almacenamiento de Respaldo en el sitio alternativo</p>	<p>El almacenamiento externo de copias de respaldo, documentación y otros recursos tecnológicos de información, catalogados como críticos, debe ser establecido para soportar el plan de recuperación y continuidad del negocio. Los propietarios de los procesos de negocio y el personal de la función IT deben involucrarse en determinar que recursos de respaldos deben ser almacenados en el sitio alternativo. La instalación de almacenamiento externo debe contar con medios ambientales para los medios y otros recursos almacenados y debe tener un nivel de seguridad suficiente que permita proteger los recursos de respaldo contra accesos no autorizados, robo o daño. La gerencia de TI debe asegurar que los acuerdos/contratos del sitio alternativo son periódicamente analizados, al menos una vez al año, para garantizar que ofrezca seguridad y protección ambiental</p>	<p>3</p>	<p>3</p>	<p>9</p>	
---	--	----------	----------	----------	--

<b>Garantizar la seguridad de sistemas</b>					
Administrar Medidas de Seguridad	La seguridad en Tecnología de Información deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. traducir información sobre evaluación de riesgos a los planes de seguridad de tecnología implementar el plan de seguridad de tecnología de información actualizar el plan de seguridad de tecnología de información para reflejar cambios en la configuración de tecnología evaluar el impacto de solicitudes de cambio en la seguridad monitorear la implementación del plan de seguridad de tecnología de información alinear los procedimientos de seguridad de tecnología de información a otras políticas y procedimientos	5	3	15	*****

<p>Identificación, Autenticación y Acceso</p>	<p>El acceso lógico y el uso de los recursos de TI deberán restringirse a través de la instrumentación de un mecanismo adecuado de autenticación de usuarios identificados y recursos asociados con las reglas de acceso. Dicho mecanismo deberá evitar que personal no autorizado, conexiones telefónicas de marcado y otros puertos de entrada del sistema (redes) tengan acceso a los recursos de cómputo, de igual forma deberá minimizar la necesidad de firmas de entrada múltiples a ser utilizadas por usuarios autorizados. Asimismo deberán establecerse procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso (por ejemplo, cambios periódicos de contraseñas o passwords).</p>	<p>4</p>	<p>3</p>	<p>12</p>	<p>*****</p>
---	---	----------	----------	-----------	--------------

Seguridad de Acceso a Datos en Línea	En un ambiente de tecnología de información en línea, la Gerencia de la función de servicios de información deberá implementar procedimientos acordes con la política de seguridad que garantiza el control de la seguridad de acceso, tomando como base las necesidades individuales demostradas de visualizar, agregar, modificar o eliminar datos.	3	3	9	
Administración de Cuentas de Usuario	La Gerencia deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario. Deberá incluirse un procedimiento de aprobación formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso.	5	3	15	*****
Vigilancia de Seguridad	La administración de seguridad de la función de servicios de información debe asegurar que la actividad de seguridad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea	5	3	15	*****

	notificada inmediatamente al administrador y que las acciones consecuentes sean tomadas en forma automática.				
Clasificación de Datos	La Gerencia deberá asegurar que todos los datos son clasificados en términos de sensibilidad, mediante una decisión explícita y formal del dueño de los datos de acuerdo con el esquema de clasificación. Aún los datos que requieran "no protección" deberán contar con una decisión formal que les asigne dicha clasificación.	5	3	15	*****
Reportes de Violación y de Actividades de Seguridad	La administración de la función de servicios de información deberá asegurar que las violaciones y la actividad de seguridad sean registradas, reportadas, revisadas y escaladas apropiadamente en forma regular para identificar y resolver incidentes que involucren actividades no autorizadas. El acceso lógico a la información sobre el registro de recursos de cómputo (seguridad y otros registros)	3	3	9	

	deberá otorgarse tomando como base el principio de menor privilegio (necesidad de saber).				
No Rechazo	Las políticas organizacionales deberán asegurar que, en donde sea apropiado, las transacciones no puedan ser negadas por ninguna de las partes y que se instrumenten controles para proporcionar no negación ( <i>non repudiation</i> ) de origen o destino, prueba de envío ( <i>proof of submission</i> ), y recibo de transacciones. Esto puede ser implementado a través de firmas digitales, registro de tiempos y terceros confiables.	3	3	9	
Sendero Seguro	Las políticas organizacionales deberán asegurar que la información de transacciones sensitivas es enviada y recibida exclusivamente a través de canales o senderos seguros ( <i>trusted paths</i> ). La información sensitiva incluye: información	3	3	9	

	sobre administración de seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas. Para lograr esto, se pueden establecer canales confiables mediante el encriptamiento entre usuarios, entre usuarios y sistemas y entre sistemas.				
Prevención, Detección y Corrección de Software "Malicioso"	Con respecto al software malicioso, tal como los virus computacionales o <i>Caballos de Troya</i> , la Gerencia deberá establecer un marco de referencia de adecuadas medidas de control preventivas, detectivas y correctivas.	3	3	9	
Arquitecturas de <i>FireWalls</i> y conexión a redes públicas	Si existe conexión con Internet u otras redes públicas en la organización. Se deberá contar con sistemas <i>Fire Wall</i> adecuados para proteger en contra de negación de servicios y cualquier acceso no autorizado a los recursos internos; deberá controlar en ambos sentidos cualquier flujo de administración de infraestructura y de aplicaciones y deberá proteger en contra de negación o ataques de servicio.	3	3	9	



Administración de datos					
Procedimientos de Preparación de Datos	La Gerencia deberá establecer procedimientos de preparación de datos a ser seguidos por los departamentos usuarios. En este contexto, el diseño de formas de entrada de datos deberá ayudar a minimizar los errores y las omisiones. Durante la creación de los datos, los procedimientos de manejo de errores deberán asegurar razonablemente que los errores y las irregularidades sean detectados, reportados y corregidos.	5	3	15	*****
Manejo de errores de documentos fuente	Los procedimientos de manejo de errores durante la creación de datos deberán asegurar razonablemente que los errores y las irregularidades sean detectados, reportados y corregidos.	4	3	12	*****
Retención de Documentos Fuente	Deberán establecerse procedimientos para asegurar que la organización pueda retener o reproducir los documentos fuentes originales durante un período de tiempo razonable para facilitar la recuperación o	5	2	10	

	reconstrucción de datos, así como para satisfacer requerimientos legales.				
Chequeos de Exactitud, Suficiencia y Autorización	Los datos sobre transacciones, capturados para su procesamiento (generados por personas, por sistemas o entradas de interfase) deberán estar sujetos a una variedad de controles para verificar su exactitud, suficiencia y validez. Asimismo, deberán establecerse procedimientos para asegurar que los datos de entrada sean validados y editados tan cerca del punto de origen como sea posible.	4	3	12	*****
Manejo de Errores en el Procesamiento de Datos	La organización deberá establecer procedimientos de manejo de errores en el procesamiento de datos que permitan la identificación de transacciones erróneas sin que éstas sean procesadas y sin interrumpir el procesamiento de otras transacciones válidas.	3	3	9	

<p>Protección de Información Sensible durante transmisión y transporte</p>	<p>La Gerencia deberá asegurar que durante la transmisión y transporte de información sensible, se proporcione una adecuada protección contra acceso o modificación no autorizada, así como contra envíos a direcciones erróneas.</p>	<p>5</p>	<p>3</p>	<p>15</p>	<p>*****</p>
<p>Responsabilidades de la Administración de la Librería de Medios</p>	<p>La Gerencia de la función de servicios de información deberá establecer procedimientos de administración para proteger el contenido de la librería de medios. Deberán definirse estándares para la identificación externa de medios magnéticos y el control de su movimiento y almacenamiento físico para soportar su seguimiento y registro. Las responsabilidades sobre el manejo de la librerías de medios (cintas magnéticas, cartuchos, discos y diskettes) deberán ser asignadas a miembros específicos del personal de servicios de información.</p>	<p>5</p>	<p>2</p>	<p>10</p>	



<p>Respaldo y Restauración</p>	<p>La Gerencia deberá implementar una estrategia apropiada de respaldo y restauración para asegurar que ésta incluya una revisión de los requerimientos del negocio, así como el desarrollo, implementación, prueba y documentación del plan de recuperación. Se deberán establecer procedimientos para asegurar que los respaldos satisfagan los requerimientos mencionados anteriormente.</p>	<p>5</p>	<p>3</p>	<p>15</p>	<p>*****</p>
<p>Almacenamiento de Respaldos</p>	<p>Los procedimientos de respaldo para los medios relacionados con tecnología de información deberán incluir el almacenamiento apropiado de los archivos de datos, del software y de la documentación relacionada, tanto dentro como fuera de las instalaciones. Los respaldos deberán ser almacenados con seguridad y las instalaciones de almacenamiento deberán ser revisadas periódicamente con respecto a la seguridad de acceso físico y la seguridad de los</p>	<p>5</p>	<p>2</p>	<p>10</p>	

	archivos de datos y otros elementos.				
<b>Administrar las instalaciones</b>					
Seguridad Física	Deberán establecerse apropiadas medidas de seguridad física y control de acceso para las instalaciones de tecnología de información de acuerdo con la política de seguridad general, incluyendo el uso de dispositivos de información fuera de las instalaciones. El acceso deberá restringirse a las personas que hayan sido autorizadas a contar con dicho acceso.	5	3	15	*****
Protección contra Factores Ambientales	La Gerencia de la función de servicios de información deberá asegurar que se establezcan y mantengan las suficientes medidas para la protección contra los factores ambientales (por ejemplo, fuego, polvo, electricidad, calor o humedad excesivos). Deberán instalarse equipo y dispositivos especializados para monitorear y controlar el ambiente.	3	3	9	

<p>Suministro Ininterrumpido de Energía</p>	<p>La Gerencia deberá evaluar regularmente la necesidad de generadores y baterías de suministro ininterrumpido de energía para las aplicaciones críticas de tecnología de información, con el fin de asegurarse contra fallas y fluctuaciones de energía. Cuando sea justificable, deberá instalarse el equipo más apropiado.</p>	<p>3</p>	<p>3</p>	<p>9</p>	
---	---	----------	----------	----------	--



**4.5.2.- EVALUACION DE CONTROLES EXISTENTES (OBJETIVOS DE CONTROL CRITICOS)**



Proceso	Evaluacion	Factores Criticos de Éxito	Indicadores Claves de Objetivo	Indicadores Claves de Desempeño
<b>Evaluar Riesgos</b>	<b>PO9</b>	<ul style="list-style-type: none"> <li>• Hay funciones y responsabilidades claramente definidas para la propiedad de la administración del riesgo y la obligación de reportar a la administración</li> <li>• Está establecida una política para definir los límites de riesgo y la tolerancia de riesgo</li> <li>• La evaluación del riesgo se efectúa observando las vulnerabilidades, amenazas y el valor de la información</li> <li>• Se mantiene información estructura de riesgos, alimentada por medio del reporte de incidentes</li> <li>• Existen responsabilidades y procedimientos para definir, acordar y financiar mejoras en la administración del riesgo</li> <li>• El foco de la evaluación es primariamente en las amenazas reales y menos en las teóricas</li> <li>• Las sesiones de lluvia de ideas y de análisis de la causa que lo origina que conduce a la identificación y mitigación del riesgo se realizan de forma rutinaria</li> <li>• Un tercero lleva a cabo una verificación de realidad de la estrategia para aumentar la objetividad y la misma es repetida a intervalos apropiados</li> </ul>	<ul style="list-style-type: none"> <li>• Mayor grado de conciencia de la necesidad de evaluaciones de riesgo</li> <li>• Menor número de incidentes causados por riesgos identificados después del hecho</li> <li>• Mayor número de riesgos identificados que han sido mitigados de manera suficiente</li> <li>• Mayor número de procesos de TI que han completado evaluaciones formales documentadas de riesgo</li> <li>• Porcentaje apropiado o número de medidas de estimación de costo efectivas de la evaluación del riesgo.</li> </ul>	<ul style="list-style-type: none"> <li>• Número de reuniones y talleres de administración del riesgo</li> <li>• Número de proyectos de mejoramiento de administración del riesgo</li> <li>• Número de mejoramientos del proceso de evaluación del riesgo</li> <li>• Nivel de financiamiento asignado a proyectos de manejo del riesgo</li> <li>• Número y frecuencia de actualizaciones a límites y políticas de riesgo publicados</li> <li>• Número y frecuencia de reportes de monitoreo del riesgo</li> <li>• Número de miembros del personal entrenado en metodología de manejo del riesgo</li> </ul>



Proceso	Objetivo de Control	Pruebas Diseño	Resultado	Pruebas Efectividad	Resultado
Identificación de Riesgos	La evaluación de riesgos deberá enfocarse al examen de los elementos esenciales de riesgo, tales como activos, amenazas, elementos vulnerables, protecciones, consecuencias y probabilidad de amenaza.	Listado de activos de información - clasificación de la información por niveles de criticidad y riesgo - se tiene conciencia del impacto que ocasionaría la pérdida de información		Se procedió a revisar los listados de activos, como están clasificados y que metodología de valoración usan para valorar el impacto y si está relacionado con los objetivos del negocio	







Proceso	Evaluación	Factores Críticos de Éxito	Indicadores Claves de Objetivo	Indicadores Claves de Desempeño
<p><b>Garantizar la seguridad de sistemas</b></p>	<p><b>DS5</b></p>	<ul style="list-style-type: none"> <li>• Está desarrollado un plan general de seguridad, el cual cubre la creación de conciencia, establece políticas y normas claras, identifica una implementación con eficiencia de costos y sostenible, y define procesos de monitoreo y ejecución</li> <li>• Hay conciencia de que un buen plan de seguridad necesita tiempo para evolucionar</li> <li>• La función de seguridad corporativa se reporta a la gerencia general y es responsable de ejecutar el plan de seguridad</li> <li>• La administración y el personal tienen un entendimiento común de los requerimientos de seguridad, las vulnerabilidades y las amenazas a la misma y entienden y aceptan sus propias responsabilidades de seguridad</li> <li>• La evaluación por terceros de la política y arquitectura de la seguridad se lleva a cabo periódicamente</li> <li>• Está definido un programa de "permiso de construcción", el cual identifica las líneas base de seguridad que tienen que ser cumplidas</li> <li>• Está establecido un programa de "licencia de conducción" para los que desarrollan, implementan y usan sistemas, haciendo cumplir la certificación de seguridad del personal</li> </ul>	<ul style="list-style-type: none"> <li>• No hay incidentes que causen mala imagen pública</li> <li>• Reporte inmediato de los incidentes críticos</li> <li>• Alineamiento de los derechos de acceso con las responsabilidades organizacionales</li> <li>• Reducción del número de nuevas implementaciones demoradas por preocupaciones de seguridad</li> <li>• Pleno cumplimiento de acuerdos y desviaciones registradas de los requerimientos mínimos de seguridad</li> <li>• Reducción del número de incidentes que involucran acceso no autorizado, pérdida o corrupción de la información</li> </ul>	<ul style="list-style-type: none"> <li>• Reducción del número de llamadas de servicio relacionadas con la seguridad, requerimientos de cambio o correcciones             <ul style="list-style-type: none"> <li>• Cantidad de tiempo improductivo causado por incidentes de seguridad</li> </ul> </li> <li>• Reducción del tiempo de atención de las solicitudes atendidas por la administración de seguridad</li> <li>• Número de sistemas sujetos a un proceso de detección de intrusos             <ul style="list-style-type: none"> <li>• Número de sistemas con capacidades de monitoreo activo</li> </ul> </li> <li>• Reducción del tiempo para investigar los incidentes de seguridad</li> <li>• Demora entre la detección, reporte y acción sobre los incidentes de seguridad             <ul style="list-style-type: none"> <li>• Número de días de entrenamiento de conocimientos de la seguridad de TI</li> </ul> </li> </ul>

Proceso	Objetivo de Control	Pruebas Diseño	Resultado	Pruebas Efectividad	Resultado
Administrar Medidas de Seguridad	La seguridad en Tecnología de Información deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. traducir información sobre evaluación de riesgos a los planes de seguridad de tecnología implementar el plan de seguridad de tecnología de información actualizar el plan de seguridad de tecnología de información para reflejar cambios en la configuración de tecnología evaluar el impacto de solicitudes de cambio en la seguridad monitorear la implementación del plan de seguridad de tecnología de información alinear los procedimientos de seguridad de tecnología de información a otras políticas y procedimientos	No existe un plan de seguridad de tecnología de la información, no se documentan ningún proceso de seguridad			



Proceso	Objetivo de Control	Pruebas Diseño	Resultado	Pruebas Efectividad	Resultado
<p>Identificación, Autenticación y Acceso</p>	<p>El acceso lógico y el uso de los recursos de TI deberá restringirse a través de la instrumentación de un mecanismo adecuado de autenticación de usuarios identificados y recursos asociados con las reglas de acceso. Dicho mecanismo deberá evitar que personal no autorizado, conexiones telefónicas de marcado y otros puertos de entrada del sistema (redes) tengan acceso a los recursos de cómputo, de igual forma deberá minimizar la necesidad de firmas de entrada múltiples a ser utilizadas por usuarios autorizados. Asimismo deberán establecerse procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso (por ejemplo, cambios periódicos de contraseñas o passwords).</p>	<p>Existe un mecanismo de autenticación de usuario tanto para el ingreso a la red de PC's, así como un mecanismo de autenticación de usuarios del sistema informático - El uso de conexiones telefónicas está supeditado al propietario de la línea aunque existe un sistema que controla el tiempo de uso por líneas aunque no identifica usuarios - El centro de cómputo está ubicado en un sitio provisional, ubicado dentro de las instalaciones de UGOP, el acceso es casi libre pueden hacerlo tanto personal del CC como auxiliares, doctores y administrativos</p>		<p>Se tomaron de una lista de empleados que nos proporcionó el departamento de nómina, se escogieron usuarios al azar que ya no laboran en el hospital y se procedió a verificar con los usuarios que ellos tenían que puedan acceder a la red interna es decir que sus logins pudieran estar activados tanto en la red como en los sistemas de aplicación</p>	



Proceso	Objetivo de Control	Pruebas Diseño	Resultado	Pruebas Efectividad	Resultado
Administración de Cuentas de Usuario	La Gerencia deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario. Deberá incluirse un procedimiento de aprobación formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso.	No existen un procedimiento documentado de administración de cuentas de usuario, estos se crean según las necesidades del sistema informatico, no existen notificación de parte de Recursos humanos de quien ingresa y quien sale de institucion o popr permisos ocasionales, los usuarios quedan activos hasta que personal de informatica se entera de que este hecho ha ocurrido			



Proceso	Objetivo de Control	Pruebas Diseño	Resultado	Pruebas Efectividad	Resultado
Vigilancia de Seguridad	La administración de seguridad de la función de servicios de información debe asegurar que esta actividad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente al administrador y que las acciones consecuentes sean tomadas en forma automática.	No existen bitacoras de acceso al CC y no existe un procedimiento documentado de control y vigilancia del CC, cualquier persona tiene acceso al CC solo con anunciarse			



Proceso	Objetivo de Control	Pruebas Diseño	Resultado	Pruebas Efectividad	Resultado
Clasificación de Datos	La Gerencia deberá asegurar que todos los datos son clasificados en términos de sensibilidad, mediante una decisión explícita y formal del dueño de los datos de acuerdo con el esquema de clasificación. Aún los datos que requieran "no protección" deberán contar con una decisión formal que les asigne dicha clasificación.	Se tiene conocimiento de que la información puede ser dividida por nivel de criticidad, se manejan procedimientos para el administrador de la base de datos como reglas de restricciones de acceso, división del ambiente de producción y desarrollo, procedimientos para los desarrolladores		No existen procedimientos formales escritos, el manejo de seguridades con respecto a la base de datos es muy básico	

Proceso	Evaluación	Factores Críticos de Éxito	Indicadores Claves de Objetivo	Indicadores Claves de Desempeño
<p><b>Administración de datos</b></p>	<p><b>DS11</b></p>	<ul style="list-style-type: none"> <li>• Los requerimientos de ingreso de datos están claramente establecidos, se les hacen valer y se les soporta por medio de técnicas automatizadas en todos los niveles, incluyendo bases de datos e interfaces de archivos</li> <li>• Las responsabilidades de los requerimientos de propiedad e integridad de los datos están claramente establecidas y aceptadas en toda la organización</li> <li>• La exactitud y los estándares de los datos están claramente comunicados e incorporados en los procesos de entrenamiento y de desarrollo de personal</li> <li>• Las normas de ingreso y de corrección de datos se hacen cumplir en el punto de ingreso</li> <li>• Las normas de integridad del ingreso, procesamiento y salida de los datos son formalizadas y ejecutadas</li> <li>• Los datos son mantenidos en suspenso hasta ser corregidos</li> <li>• Se usan métodos efectivos de detección para hacer que se cumplan las normas de exactitud y de integridad de datos</li> <li>• La traducción efectiva de datos en todas las plataformas está implementada sin pérdida de integridad o confiabilidad para satisfacer las exigencias cambiantes del negocio</li> </ul>	<ul style="list-style-type: none"> <li>• Una reducción que se mide en el proceso de preparación de datos y en las tareas</li> <li>• Un mejoramiento que se mide en la calidad, línea de tiempo y disponibilidad de datos</li> <li>• Un aumento que se mide en la satisfacción del cliente y en la confianza en los datos</li> <li>• Una disminución que se mide en las actividades correctivas y en la exposición a la corrupción de datos</li> <li>• Reducción del número de defectos de datos, como por ejemplo la redundancia, la duplicación y la inconsistencia</li> <li>• No hay conflictos legales o regulatorios de cumplimiento de los datos</li> </ul>	<ul style="list-style-type: none"> <li>• Una reducción que se mide en el proceso de preparación de datos y en las tareas</li> <li>• Un mejoramiento que se mide en la calidad, línea de tiempo y disponibilidad de datos</li> <li>• Un aumento que se mide en la satisfacción del cliente y en la confianza en los datos</li> <li>• Una disminución que se mide en las actividades correctivas y en la exposición a la corrupción de datos</li> <li>• Reducción del número de defectos de datos, como por ejemplo la redundancia, la duplicación y la inconsistencia</li> <li>• No hay conflictos legales o regulatorios de cumplimiento de los datos</li> </ul>



Proceso	Objetivo de Control	Pruebas Diseño	Resultado	Pruebas Efectividad	Resultado
Procedimientos de Preparación de Datos	<p>La Gerencia deberá establecer procedimientos de preparación de datos a ser seguidos por los departamentos usuarios. En este contexto, el diseño de formas de entrada de datos deberá ayudar a minimizar los errores y las omisiones. Durante la creación de los datos, los procedimientos de manejo de errores deberán asegurar razonablemente que los errores y las irregularidades sean detectados, reportados y corregidos.</p>	<p>Existía un mecanismo por el cual la información inicial como datos de filiación eran llenado en un formulario que luego era ingresado en el sistema, luego cuando el sistema alcanzo estabilidad se elimino el mecanismo, actualmente no existe ningun control para preparar los datos antes de ser ingresados al sistema informatico, los cuales son ingresados directamente en el sistema cuando el paciente llega a la ventanilla de admision o con los medicos</p>			

Proceso	Objetivo de Control	Pruebas Diseño	Resultado	Pruebas Efectividad	Resultado
Manejo de errores de documentos fuente	<p>Los procedimientos de manejo de errores durante la creación de datos deberán asegurar razonablemente que los errores y las irregularidades sean detectados, reportados y corregidos.</p>	<p>No existe un procedimiento formal para el manejo de errores en los documentos fuentes, cuando ocurre un error este es comunicado verbalmente a informatica para luego ser corregido</p>			



Proceso	Objetivo de Control	Pruebas Diseño	Resultado	Pruebas Efectividad	Resultado
Chequeos de Exactitud, Suficiencia y Autorización	Los datos sobre transacciones, capturados para su procesamiento (generados por personas, por sistemas o entradas de interfase) deberán estar sujetos a una variedad de controles para verificar su exactitud, suficiencia y validez. Asimismo, deberán establecerse procedimientos para asegurar que los datos de entrada sean validados y editados tan cerca del punto de origen como sea posible.	Las pruebas sobre exactitud y validez de los datos en las transacciones se realizan a posteriori, si existen errores estos son corregidos por el personal de informática en la mayoría de los casos y cuando estos son detectados			

Proceso	Objetivo de Control	Pruebas Diseño	Resultado	Pruebas Efectividad	Resultado
Protección de Información Sensible durante transmisión y transporte	La Gerencia deberá asegurar que durante la transmisión y transporte de información sensible, se proporcione una adecuada protección contra acceso o modificación no autorizada, así como contra envíos a direcciones erróneas.	El respaldo de información se lo realiza periódicamente, una copia queda físicamente en medios magnéticos (CD's de respaldo) y otra en la máquina del administrador de la base de datos		Se comprobó físicamente que las copias estaban en los lugares indicados	



Proceso	Objetivo de Control	Pruebas Diseño	Resultado	Pruebas Efectividad	Resultado
Respaldo y Restauración	La Gerencia deberá implementar una estrategia apropiada de respaldo y restauración para asegurar que ésta incluya una revisión de los requerimientos del negocio, así como el desarrollo, implementación, prueba y documentación del plan de recuperación. Se deberán establecer procedimientos para asegurar que los respaldos satisfagan los requerimientos mencionados anteriormente.	Existe un mecanismo de respaldo automatico que se ejecuta alas 11:00 en la noche, estos se prueban semanalmente cuando se reemplaza en el ambiente de desarrollo		Se procedió a comprobar mediante registros de auditoria , que el proceso de respaldo se ejecuta diariamente a la hora indicada, de igual manera se tomó un respaldo anterior y se lo paso a desarrollo para verificar que estaba el respaldo sin daño.	

Proceso	Evaluación	Factores Críticos de Éxito	Indicadores Claves de Objetivo	Indicadores Claves de Desempeño
<p><b>Administrar las instalaciones</b></p>	<p><b>DS12</b></p>	<ul style="list-style-type: none"> <li>• Están definidas estrategias y normas para todas las instalaciones, que abarcan la selección del sitio, la construcción, custodia, seguridad de personal, sistemas mecánico y eléctrico, protección contra incendio, rayo e inundación</li> <li>• La estrategia y las normas de las Instalaciones están alineadas con los objetivos de disponibilidad de los servicios de TI y con las políticas de seguridad de información, y están integradas con la planeación de continuidad del negocio y con la administración de crisis</li> <li>• Las Instalaciones son monitoreadas regularmente usando sistemas automatizados con tolerancias claras y logs de auditoría, CCTV (Circuito Cerrado de Televisión ) y sistemas de detección de intrusos donde es necesario, así como también a través de inspecciones físicas y auditorías</li> <li>• Hay un cumplimiento estricto de los programas de mantenimiento preventivo y estricta disciplina en el mantenimiento de las Instalaciones</li> </ul>	<ul style="list-style-type: none"> <li>• Una reducción en el número de incidentes de seguridad física instalaciones , incluyendo robo, daños, revelación, cortes de energía, salud, y problemas de seguridad</li> <li>• Una reducción en la cantidad de tiempo improductivo debido a cortes de energía en las instalaciones</li> <li>• Un cumplimiento medido de las leyes y reglamentaciones aplicables</li> <li>• Una adherencia medida a los requerimientos de políticas de seguro</li> <li>• Un mejoramiento medido en la proporción costo /riesgo</li> </ul>	<ul style="list-style-type: none"> <li>• Inventario completo y mapas con identificación de puntos únicos de falla</li> <li>• Frecuencia de entrenamiento de personal en seguridad, Instalaciones y medidas de seguridad</li> <li>• Frecuencia de prueba de alarma de incendio y planes de evacuación</li> <li>• Frecuencia de inspecciones físicas</li> <li>• Reducción del número de accesos no autorizados a salas de equipos restringidas</li> <li>• Cambio transparente y regular que garantiza que no habrá interrupción de energía</li> <li>• Demora entre el registro y la finalización de incidentes físicos</li> </ul>

Proceso	Objetivo de Control	Pruebas Diseño	Resultado	Pruebas Efectividad	Resultado
Seguridad Física	Deberán establecerse apropiadas medidas de seguridad física y control de acceso para las instalaciones de tecnología de información de acuerdo con la política de seguridad general, incluyendo el uso de dispositivos de información fuera de las instalaciones. El acceso deberá restringirse a las personas que hayan sido autorizadas a contar con dicho acceso.	Existen guardias que anotan en una bitacora quien ingresa para llevar el control de la gente que ingresa a las instalaciones y se debe revisar con que salen tanto las visitas como el personal		Se solicito revisar las bitacoras que manejan los guardias asi como el procedimiento.No existe un procedimiento documentado que garantice que se cumplen normas de seguridad fisica, no se cumple el control de revisar que traen, hacia donde va, cual es el motivo, asi mismo cuando sale de las instalaciones no se realiza una revision de que lleva en el momento de su salida	

## CAPITULO 5

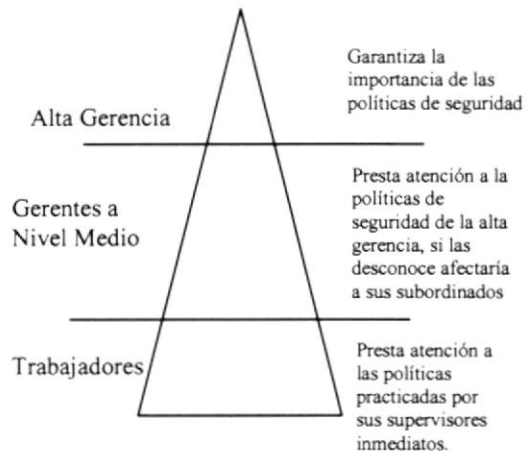
### POLÍTICAS GENERALES

#### 5.1.- GENERALIDADES

La información es un recurso que, como el resto de los activos, tiene valor para la Institución y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Hospital.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.



Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades de la Institución y Gerencias Medias para la difusión, consolidación y cumplimiento de la presente Política.

#### 5.2.- OBJETIVO

Proteger los recursos de información del Hospital y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales,

con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando sus recursos, sin que ello implique necesariamente la asignación de partidas adicionales.

Mantener la Política de Seguridad del Hospital actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

### **5.3.- ALCANCE**

Esta Política se aplica en todo el ámbito del Hospital, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

### **5.4.- RESPONSABILIDAD**

Todos los Directores Generales, Gerentes o equivalentes, Responsables de áreas tanto se trate de administrativas o personal técnico y sea cual fuere su nivel jerárquico son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal del Hospital, cualquiera sea su situación, el área a la cual se encuentre afectada y cualquiera sea el nivel de las tareas que desempeñe.

Las máximas autoridades del Hospital aprueban esta Política y son responsables de la autorización de sus modificaciones.

**5.4.1.- La persona encargada de Seguridad de la Información** del Hospital, procederá a revisar y proponer a la máxima autoridad para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información. Debe garantizar que la seguridad sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios;

promover la difusión y apoyo a la seguridad de la información y coordinar el proceso de administración de la continuidad de las actividades del Hospital.

**5.4.2.- El Gerente del Área de Tecnología** cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Institución. Por otra parte tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

**5.4.3.- Los Propietarios de la Información** son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

**5.4.4.- El Coordinador de Recursos Humanos** o quién desempeñe esas funciones, cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continúan en materia de seguridad.

**5.4.5.- El Responsable del Área Legal** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la Institución con sus empleados y con terceros. Asimismo, asesorará en materia legal al Organismo, en lo que se refiere a la seguridad de la información.

**5.4.6.- Los usuarios de la información** y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

El Organismo debe tener un completo conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

- • Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.
- • Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.
- • Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.
- • Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.). Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para el Organismo.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos.

Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información. Por último, la información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

#### **5.5.- OBJETIVO**

Garantizar que los activos de información reciban un apropiado nivel de protección. Clasificar la información para señalar su sensibilidad y criticidad. Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

#### **5.6.- ALCANCE**

Esta Política se aplica a toda la información administrada en el Organismo, cualquiera sea el soporte en que se encuentre.

#### **5.7.- RESPONSABILIDAD**

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente Política.



## **5.8.- POLÍTICA INVENTARIO DE ACTIVOS**

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 6 meses.

El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa.

## **5.9.- CLASIFICACIÓN DE LA INFORMACIÓN**

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

A continuación se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

- Confidencialidad:
  - 0- Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado O NO de la organización
  - 1- Información que puede ser conocida y utilizada por todos los empleados del Organización, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la organización
  - 2- Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la organización.
  - 3- Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la organización, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves a la organización.
  
- Integridad:
  - 0- Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria de la organización.

1- Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para la organización.

2- Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la organización.

3- Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a la organización.

- Disponibilidad:

0- Información cuya inaccesibilidad no afecta la operatoria de la organización.

1- Información cuya inaccesibilidad permanente durante... (Definir un plazo no menor a una semana) podría ocasionar pérdidas significativas para la organización.

2- Información cuya inaccesibilidad permanente durante.... (Definir un plazo no menor a un día) podría ocasionar pérdidas significativas a la organización.

3- Información cuya inaccesibilidad permanente durante..... (Definir un plazo no menor a una hora) podría ocasionar pérdidas significativas a la organización.

Al referirse a pérdidas, se contemplan aquellas mesurables (materiales) y no mesurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

- **CRITICIDAD BAJA:** ninguno de los valores asignados superan el 1.
- **CRITICIDAD MEDIA:** alguno de los valores asignados es 2
- **CRITICIDAD ALTA:** alguno de los valores asignados es 3

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al depositario del recurso.

- Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deberán tener acceso a la misma.

En adelante se mencionará como "información clasificada" (o "datos clasificados") a aquella que se encuadre en los niveles 1, 2 o 3 de Confidencialidad.

#### **5.10.- ROTULADO DE LA INFORMACIÓN**

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- Copia
- Almacenamiento
- Transmisión por correo, fax, correo electrónico
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.).

### 5.11.- PLAN DE APLICABILIDAD

Luego de la identificación de potenciales riesgos, amenazas y vulnerabilidades se pudo determinar el conjunto de actividades más importantes a ser realizadas por el Personal del Sistema Hospitalario Docente de la Universidad de Guayaquil, estas actividades permitirán alinear las medidas de seguridad existentes con las exigidas por las Políticas de Seguridad elaboradas.

Las actividades a ser realizadas en el Sistema Hospitalario Docente de la Universidad de Guayaquil son las siguientes:

- Clasificación de la Información
- Inventario de usuarios y accesos a los sistemas
- Seguridad de red y comunicaciones
- Campaña de concientización de usuarios
- Verificación y adaptación de los sistemas del Hospital a la Política planteada
- Estandarización de la configuración del software base
- Revisión y adaptación de procedimientos complementarios (Procesos evaluativos de control de calidad)

Para cada actividad se ha elaborado una breve descripción del objetivo que se cubrirá al aplicar la actividad, las tareas a ser desarrolladas por etapas, la relación de precedencia y secuencia que presenta con otras actividades y un tiempo estimado de duración. El tiempo estimado para el desarrollo de cada etapa debe ser revisado antes de iniciar la misma y puede sufrir variaciones de acuerdo a dicha evaluación final y/o criterio de las personas evaluadoras del proceso.

### CLASIFICACIÓN DE LA INFORMACIÓN

<b>Tiempo estimado</b>	10 semanas
<b>Objetivo</b>	Proteger los activos de información
<b>Actividades</b>	Realizar un proyecto para la clasificación de la información utilizada por las distintas unidades de negocio, mediante la cual se podrán definir los recursos apropiados y necesarios Para proteger los activos de información. El objetivo de la clasificación es priorizar la utilización de recursos para aquella información que requiere de mayores niveles de protección. Los criterios a ser empleados para la clasificación

	de la información son los siguientes:
<b>Observaciones</b>	<p>Información restringida (R)                  Información con mayor grado de sensibilidad, el acceso a esta información debe ser analizado y autorizado caso por caso.</p> <p>Información Confidencial (C)                  Información sensible que solo debe ser conocida y divulgada a personas que la necesiten para el cumplimiento de las funciones encomendadas dentro de la institución.</p> <p>Información de Uso Interno (I)                  Son datos y/o información generada al interior de la organización que permite facilitar las operaciones diarias, debe ser administrada por personal de la organización, pero no requiere medidas complejas de seguridad.</p> <p>Información General (G)                  Información que esta disponible al publico en general</p>

### INVENTARIO DE ACTIVOS

<b>Tiempo estimado</b>	10 semanas
<b>Objetivo</b>	Identificar a los usuarios de la información
<b>Actividades</b>	Realizar un control que permita documentar los activos de información sensibles y no sensibles; así como los responsables de custodiar tanto el equipo como la información almacenada en ellos. Los criterios a ser empleados para la creación de este control son los siguientes:
<b>Observaciones</b>	<p>Información almacenada en cualquier medio de almacenamiento, inclusive la información impresa.</p> <p>Definición de los responsables de custodiar los activos identificados.</p> <p>Clasificación de la información por parte de los responsables definidos.</p> <p>Consolidación de los activos de información, así como los custodios identificados.</p> <p>Determinación de las medidas de seguridad a ser aplicados para cada activo identificado.</p> <p>Implementación de medidas de seguridad determinadas</p>

	previamente.
--	--------------

### INVENTARIO DE ACCESO A LOS SISTEMAS

<b>Tiempo estimado</b>	10 semanas
<b>Objetivo</b>	Controlar los accesos a la información sensible
<b>Actividades</b>	Realizar un control que permita identificar los acceso de los usuarios a los sistemas del Sistema Hospitalario, se debe realizar un inventario de todos los accesos que poseen sobre cada uno de los sistemas. Este inventario debe ser actualizado al modificar el perfil de acceso de algún usuario y será utilizado para realizar revisiones periódicas de los accesos otorgados en los sistemas. Los criterios a ser empleados para la creación de este control son los siguientes:
<b>Observaciones</b>	Elaboración de un inventario de las aplicaciones y sistemas informáticos del Sistema Hospitalario. Elaboración de un inventario de los perfiles de acceso a sistema y de los usuarios involucrados. Verificación de los perfiles definidos en los sistemas para cada usuario y compararlo con la función que cumplen dentro de la organización. Revisión y aprobación de los accesos por parte de las gerencias de área respectivas. Depurar los perfiles de acceso de los usuarios a los sistemas. Mantenimiento periódico de este inventario.

### SEGURIDAD EN REDES Y COMUNICACIONES

<b>Tiempo estimado</b>	8 semanas
<b>Objetivo</b>	Controlar el uso indebido de equipos locales y de comunicación
<b>Actividades</b>	Controlar el uso de equipos de comunicación por personal no autorizado y garantizar que la configuración que poseen brinde mayor seguridad y eficiencia a las comunicaciones, se requiere que los equipos que soportan dicho servicio, se encuentren adecuadamente configurados. Los criterios a ser

	empleados para la creación de este control son los siguientes:
<b>Observaciones</b>	<p>Elaboración de un inventario de equipos de comunicación (routers, switch, firewall, etc.).</p> <p>Elaboración de estándares de configuración para los equipos de comunicación.</p> <p>Evaluación de funcionamiento de los equipos identificados.</p> <p>Adaptación de la infraestructura de red existente a las necesidades de la organización.</p> <p>Implementar un sistema de Antivirus para servicios de Internet (SMTP, FTP, HTTP).</p> <p>Implementar un gateway antivirus de servicios de Internet, a través del cual pasarán las comunicaciones establecidas entre la red interna e Internet.</p> <p>Implementar un sistema de monitoreo de Intrusos para detectar los intentos de intrusión o ataque desde redes externas hacia la red de datos de la organización.</p> <p>Evaluación de seguridad de la red y aplicación de controles de ser necesarios. Verificación de la configuración de:</p> <ul style="list-style-type: none"> <li>- Servidor Proxy (Internet)</li> <li>- Firewall</li> <li>- Servidor de correo electrónico (correo interno)</li> </ul> <p>Mantenimiento periódico de los inventarios establecidos.</p>

### **CAMPAÑA DE CONCIENTIZACION DE USUARIOS**

<b>Tiempo estimado</b>	20 semanas
<b>Objetivo</b>	Lograr un compromiso y concientización de los usuarios en temas relacionados con seguridad.
<b>Actividades</b>	Con el objetivo de lograr un compromiso de los usuarios en temas referentes a seguridad de información de la organización, se debe realizar una campaña de concientización del personal la cual esté orientada a dar a conocer al personal conceptos básicos de seguridad y a grupos específicos temas correspondientes a sus responsabilidades en la organización. Los criterios a ser empleados para la lograr este objetivo son los siguientes:
<b>Observaciones</b>	Definición del mensaje a transmitir y el material o medio de

	<p>difusión empleado para los distintos grupos de usuarios, entre ellos:</p> <p>Personal en general: información general sobre seguridad, políticas y estándares incluyendo protección de virus, contraseñas, seguridad física, sanciones, correo electrónico y uso de Internet.</p> <p>Personal de Sistemas: Políticas de seguridad, estándares y controles específicos para la tecnología y aplicaciones utilizadas.</p> <p>Gerencias y jefaturas: Monitoreo de seguridad, responsabilidades de supervisión, políticas de sanción. Identificación del personal de cada departamento que se encargará de actualizar a su propio grupo en temas de seguridad.</p> <p>Establecimiento de un cronograma de capacitación, el cual debe incluir, empleados nuevos, requerimientos anuales de capacitación, actualizaciones.</p> <p>Desarrollo el cronograma de presentaciones.</p> <p>Realizar la campaña según el cronograma elaborado, asegurándose de mantener un registro actualizado de la capacitación de cada usuario.</p>
--	---

**VERIFICACIÓN Y ADAPTACIÓN DE LOS SISTEMAS A LA POLÍTICA DE SEGURIDAD PLANTEADA**

<b>Tiempo estimado</b>	12 semanas
<b>Objetivo</b>	Asegurar el cumplimiento de la Política de Seguridad propuesta.
<b>Actividades</b>	Con el objetivo de lograr seguridad en los controles existentes, se debe verificar el grado de cumplimiento de las políticas de seguridad en los sistemas y adaptarlos en caso de verificar su incumplimiento. Los criterios a ser empleados para la lograr este objetivo son los siguientes:
<b>Observaciones</b>	Elaboración de un inventario de los sistemas existentes (propuesto anteriormente), incluyendo los servicios brindados a clientes como parte de ciclo de atención medica. Elaboración de un resumen de los requisitos que deben cumplir las aplicaciones según la política y estándares de



	<p>seguridad.</p> <p>Evaluación del grado de cumplimiento de la política de seguridad para cada una de las aplicaciones existentes y la viabilidad de su modificación para cumplir con la política de seguridad, elaborando la relación de cambios que deben ser realizados en cada aplicación.</p> <p>Adaptación de los sistemas a la política de seguridad (diseño, desarrollo, pruebas, actualización de la documentación, etc.).</p> <p>Estandarización de controles para contraseñas de los sistemas.</p> <p>Los sistemas no requerirán modificaciones si su adaptación no es viable.</p> <p>Pase a producción de sistemas adaptados.</p>
--	--

#### **ESTANDARIZACIÓN DE LA CONFIGURACIÓN DEL SOFTWARE BASE.**

<b>Tiempo estimado</b>	10 semanas
<b>Objetivo</b>	Proteger adecuadamente la información.
<b>Actividades</b>	<p>Con el objetivo de lograr seguridad en los servidores y computadores personales, se debe realizar una adecuada configuración de los parámetros de seguridad del software base que soporta las aplicaciones de la organización. Los criterios a ser empleados para la lograr este objetivo son los siguientes:</p>
<b>Observaciones</b>	<p>Elaboración de un inventario de sistemas operativos de Servidores y computadores personales.</p> <p>Elaboración de estándares de configuración para Windows XP Professional, Windows 2000 Professional, SQL Server.</p> <p>Elaboración de un inventario de bases de datos existentes.</p> <p>Evaluación de los de sistemas identificados.</p> <p>Adaptación del software base a la política de seguridad.</p>

**REVISIÓN Y ADAPTACIÓN DE PROCEDIMIENTOS COMPLEMENTARIOS  
(PROCESOS EVALUATIVOS DE CONTROL DE CALIDAD)**

<b>Tiempo estimado</b>	12 semanas
<b>Objetivo</b>	Adoptar procedimientos de Control Complementario.
<b>Actividades</b>	Con el objetivo de lograr que las actividades propuestas se cumplan con lo estipulado en la Política de Seguridad. Los criterios a ser empleados para la lograr este objetivo son los siguientes:
<b>Observaciones</b>	<p>Elaboración de procedimientos de monitoreo, incluyendo procedimientos para verificación periódica de carpetas compartidas, generación de copias de respaldo de información de usuarios, aplicación de controles de seguridad para información en computadores portátiles, etc.</p> <p>Elaboración de procedimientos de monitoreo y reporte sobre la administración de los sistemas y herramientas de seguridad, entre ellas: antivirus, servidores de seguridad del contenido, servidor Proxy, servidor firewall, sistema de detección de intrusos.</p> <p>Establecimiento de controles para la información transmitida a clientes y usuarios de los sistemas.</p> <p>Revisión y establecimiento de controles para el almacenamiento físico de información.</p> <p>Revisión y establecimiento de controles para personal que realiza labores utilizando activos de información de la organización (Soporte Técnico, Limpieza, mantenimiento, etc.)</p>

**PLAN DE APLICABILIDAD**

ACTIVIDAD	MESES												
	1	2	3	4	5	6	7	8	9	10	11	12	
Realizar un proyecto para la clasificación de la información utilizada por las distintas unidades de negocio.	■	■	■										
Realizar un control que permita documentar los activos de información sensibles y no sensibles.			■	■	■								
Realizar un control que permita identificar los accesos de los usuarios a los sistemas del Sistema Hospitalario.				■	■	■							
Controlar el uso de equipos de comunicación no autorizado y garantizar que la configuración brinde mayor seguridad y eficiencia a las comunicaciones.					■	■	■						
Realizar una campaña de concientización del personal la cual esté orientada a dar a conocer al personal conceptos de seguridad y su implicación.				■	■	■	■	■					
Verificar el grado de cumplimiento de las políticas de seguridad en los sistemas y adaptarlos en caso de verificar su incumplimiento.							■	■	■				
Realizar una adecuada configuración de los parámetros de seguridad del software base que soporta las aplicaciones de la organización.								■	■	■	■		
Verificar que las actividades propuestas se cumplan con lo estipulado en la Política de Seguridad.											■	■	■

**NOTA: LA DURACIÓN DE LOS PROYECTOS ESTÁ SUJETA A VARIACIONES DEPENDIENTES A LA SITUACIÓN EXISTENTE Y EL ANÁLISIS REALIZADO PREVIO A CADA ACTIVIDAD.**

## **CAPITULO 6.- POLITICAS ESPECIFICAS**

### **6.1.- CONTROL DE ACCESOS**

#### **6.1.1.- GENERALIDADES**

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concienciar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

#### **6.1.2.- OBJETIVOS**

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de la organización y otras redes públicas o privadas.
- Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

- Concienciar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

### **6.1.3.- ALCANCE**

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información de la organización, cualquiera sea la función que desempeñe.

Así mismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

### **6.1.4.- RESPONSABILIDAD**

El Responsable de Seguridad Informática estará a cargo de:

- Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades; y el ajuste de relojes de acuerdo a un estándar preestablecido.
- Definir pautas de utilización de Internet para todos los usuarios.
- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, ruteadores o gateways, etc.) y validarlos periódicamente.
- Controlar la asignación de privilegios a usuarios.

- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registro de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos, subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.
- Concienciar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.
- Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información con el objeto de:
  - determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
  - definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.
- Aprobar y solicitar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.

- Definir un cronograma de depuración de registros de auditoría en línea.

Los Propietarios de la Información junto con Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

Los Responsables de las Unidades Organizativas, junto con el Responsable de Seguridad Informática, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes. Asimismo autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

El Responsable del Área Informática o un delegado de él cumplirán las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Evaluar el costo y el impacto de la implementación de "enrutadores" o "gateways" Adecuados para subdividir la red y recomendar el esquema apropiado.
- Implementar el control de puertos, de conexión a la red y de ruteo de red.
- Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.
- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.

- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de Control de Accesos como identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).
- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.
- Efectuar un control de los registros de auditoria generados por los sistemas operativos y de comunicaciones.

La Unidad de Auditoria Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

## **6.2.- POLÍTICA DE CONTROL DE ACCESOS**

En la aplicación de controles de acceso, se contemplarán los siguientes aspectos:

- Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- Identificar toda la información relacionada con las aplicaciones.
- Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información.
- Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.



- Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
- Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

### **6.2.1.- REGLAS DE CONTROL DE ACCESO**

Las reglas de control de acceso especificadas, deberán:

- Indicar expresamente si las reglas son obligatorias u optativas
- Establecer reglas sobre la premisa "Todo debe estar prohibido a menos que se permita expresamente" y no sobre la premisa inversa de "Todo está permitido a menos que se prohíba expresamente".
- Controlar los cambios en los rótulos de información que son iniciados automáticamente por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario.
- Controlar los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.
- Controlar las reglas que requieren la aprobación del administrador o del propietario de la Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

### **6.2.2.- ADMINISTRACIÓN DE ACCESOS DE USUARIOS**

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

### **6.2.3.- REGISTRO DE USUARIOS**

El Responsable de Seguridad Informática definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

- Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
- Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
- Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad de la organización, por ejemplo que no compromete la segregación de tareas.
- Entregar a los usuarios un detalle escrito de sus derechos de acceso.
- Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
- Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
- Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la Organización o sufrieron la pérdida/robo de sus credenciales de acceso.
- Efectuar revisiones periódicas con el objeto de:
  - cancelar identificadores y cuentas de usuario redundantes

- inhabilitar cuentas inactivas por más de un plazo establecido (indicar período no mayor a 60 días)
- eliminar cuentas inactivas por más de un plazo establecido (indicar período no mayor a 120 días)
  
- En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.
  
- Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
  
- Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

#### **6.2.4.- ADMINISTRACIÓN DE PRIVILEGIOS**

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

- Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
  
- Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
  
- Mantener un proceso de autorización y un registro de todos los privilegios asignados.

- Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
- Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.
- Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.
- Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad Informática.

#### **6.2.5.- ADMINISTRACIÓN DE CONTRASEÑAS DE USUARIO**

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

- Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad.
- Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
- Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.
- Almacenar las contraseñas sólo en sistemas informáticos protegidos.

- Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica (por ejemplo verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (como las tarjetas de circuito integrado), etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el Responsable de Seguridad Informática conjuntamente con el Responsable del Área de Informática y el Propietario de la Información lo determine necesario (o lo justifique).
  
- Configurar los sistemas de tal manera que:
  - las contraseñas tengan un formato definido (especificar cantidad no menor a 8 caracteres)
  - suspendan o bloqueen permanentemente al usuario luego de tiempo determinado (especificar cantidad no mayor a 3) intentos de entrar con una contraseña incorrecta (deberá pedir la rehabilitación ante quien corresponda),
  - solicitar el cambio de la contraseña cada periodo establecido (especificar lapso no mayor a 45 días)
  - impedir que las últimas contraseñas (especificar cantidad no menor a 12 contraseñas) no sean reutilizadas,
  - establecer un tiempo de vida mínimo establecido (especificar cantidad no mayor a 3 días para las contraseñas).

#### **6.2.6.- ADMINISTRACIÓN DE CONTRASEÑAS CRÍTICAS**

En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Responsable de Seguridad Informática definirá procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

- Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido.
- Las contraseñas seleccionadas serán seguras, y su definición será efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa.
- Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
- La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.
- Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado.
- Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el Responsable de Seguridad.

#### **6.2.7.- REVISIÓN DE DERECHOS DE ACCESO DE USUARIOS**

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate llevará a cabo un proceso formal, a intervalos regulares (indicar periodicidad no mayor a 6 meses), a fin de revisar los derechos de acceso de los usuarios. Se deberán contemplar los siguientes controles:

- Revisar los derechos de acceso de los usuarios a intervalos de tiempo (especificar tiempo no mayor a 6 meses).
- Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de tiempo (especificar tiempo no mayor a 3 meses).

- Revisar las asignaciones de privilegios a intervalos de tiempo (especificar tiempo no mayor a 6 meses), a fin de garantizar que no se obtengan privilegios no autorizados.

## **6.2.8.- RESPONSABILIDADES DEL USUARIO**

### **6.2.8.1.- USO DE CONTRASEÑAS**

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

- Mantener las contraseñas en secreto.
- Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:
  - Sean fáciles de recordar.
  - No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
  - No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- Cambiar las contraseñas provisionales en el primer inicio de sesión ("log on").

- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- Notificar de acuerdo a lo establecido en "Incidentes Relativos a la Seguridad", cualquier incidente de seguridad relacionado con sus contraseñas sea esto pérdida, robo o indicio de pérdida de confidencialidad.
- Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.



## **6.3.- SEGURIDAD FÍSICA Y AMBIENTAL**

### **6.3.1.- GENERALIDADES**

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible de la organización, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones de la organización como en instalaciones próximas a la sede del mismo que puedan interferir con las actividades.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas de la organización. Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de Preservación de la información almacenada en los mismos. Así también se tendrá en cuenta la Aplicación de dichas normas en equipamiento perteneciente al Organismo pero situado físicamente fuera del mismo ("housing") así como en equipamiento ajeno que albergue Sistemas y/o preste servicios de procesamiento de información al Organismo ("hosting").

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados.

Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación.

### **6.3.2.- OBJETIVOS**

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información de la organización.

Proteger el equipamiento de procesamiento de información crítica de la organización ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de la organización.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales. Proporcionar protección proporcional a los riesgos identificados.

### **6.3.3.- ALCANCE**

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información de la organización: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

### **6.3.4.- RESPONSABILIDAD**

El Responsable de Seguridad Informática definirá junto con el Responsable del Área Informática y los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas.

El Responsable del Área Informática asistirá al Responsable de Seguridad Informática en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones de la organización.

Los Responsables de Unidades Organizativas definirán los niveles de acceso físico del personal de la organización a las áreas restringidas bajo su responsabilidad.

Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los empleados de la organización cuando lo crean conveniente.

La Unidad de Auditoria Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información revisará los registros de acceso a las áreas protegidas.

Todo el personal de la organización es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

#### **6.4.- POLÍTICA PERÍMETRO DE SEGURIDAD FÍSICA**

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes de la organización y de las instalaciones de procesamiento de información.

El Organismo utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, aire acondicionado, respaldo de información y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información de la organización.

Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas.

El emplazamiento y la fortaleza de cada barrera estarán definidas por el Responsable del Área Informática con el asesoramiento del Responsable de Seguridad Informática.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

- Definir y documentar claramente el perímetro de seguridad.
- Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción).
- Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo mediante mecanismos de control, vallas, alarmas, cerraduras, etc.
- Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán los siguientes medios alternativos de control de acceso físico al área o edificio (indicar otros medios alternativos de control). El acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.
- Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.
- Identificar claramente todas las puertas de incendio de un perímetro de seguridad.
- El Responsable de Seguridad Informática llevará un registro actualizado de los sitios protegidos, indicando:
  - Identificación del Edificio y Área.
  - Principales elementos a proteger.
  - Medidas de protección física.

#### **6.4.1.- CONTROLES DE ACCESO FÍSICO**

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad Informática junto con el Responsable del Área Informática, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

- Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
- Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán los siguientes controles de autenticación para autorizar y validar todos los accesos (por ejemplo: personal de guardia con listado de personas habilitadas o por tarjeta magnética o inteligente y número de identificación personal (PIN), etc.). Se mantendrá un registro protegido para permitir auditar todos los accesos.
- Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.
- Revisar y actualizar cada cierto tiempo (definir período no mayor a 6 meses) los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Responsable de la Unidad Organizativa de la que dependa.
- Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

#### **6.4.2.- PROTECCIÓN DE OFICINAS E INSTALACIONES**

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad.

Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se definen los siguientes sitios como áreas protegidas de la organización y Se establecen las siguientes medidas de protección para áreas protegidas:

- Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
- Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
- Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.
- Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.
- Implementar los siguientes mecanismos de control para la detección de intrusos, los mismos serán instalados según estándares profesionales y probados periódicamente. Estos mecanismos de control comprenderán todas las puertas exteriores y ventanas accesibles.
- Separar las instalaciones de procesamiento de información administradas por el Organismo de aquellas administradas por terceros.

- Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.
- Almacenar los materiales peligrosos o combustibles en los siguientes lugares seguros a una distancia prudencial de las áreas protegidas de la organización (lugares seguros). Los suministros, como los útiles de escritorio, no serán trasladados al área protegida hasta que sean requeridos.
- Almacenar los equipos redundantes y la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal (detallar ubicación).

#### **6.4.3.- DESARROLLO DE TAREAS EN ÁREAS PROTEGIDAS**

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

- Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
- Evitar la ejecución de trabajos por parte de terceros sin supervisión.
- Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.
- Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.

- Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.
- Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el Responsable de dicho área o el Responsable del Área Informática y el Responsable de Seguridad Informática.
- Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

#### **6.4.4.- AISLAMIENTO DE LAS ÁREAS DE RECEPCIÓN Y DISTRIBUCIÓN**

Se controlarán las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

- Limitar el acceso a las áreas de depósito, desde el exterior de la sede de la organización, sólo al personal previamente identificado y autorizado.
- Diseñar el área de depósito de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.
- Proteger todas las puertas exteriores del depósito cuando se abre la puerta interna.
- Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.
- Registrar el material entrante al ingresar al sitio pertinente.



#### **6.4.5.- UBICACIÓN Y PROTECCIÓN DEL EQUIPAMIENTO Y COPIAS DE SEGURIDAD**

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

- Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
- Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
- Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
- Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por Amenazas Potenciales Controles (Robo o hurto, Incendio, Explosivos, Humo, Inundaciones o filtraciones de agua o falta de suministro, Polvo, Vibraciones, Efectos químicos, Interferencia en el suministro de energía eléctrica, variación de tensión, Radiación electromagnética, Derrumbes)
- Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará cada cierto tiempo (indicar periodicidad, no mayor a seis meses).
- Considerar asimismo el impacto de las amenazas citadas en el punto d) que tengan lugar en zonas próximas a la sede de la organización.

#### **6.4.6.- SUMINISTROS DE ENERGÍA**

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

- Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
- Contar con un suministro de energía ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la organización. La determinación de dichas operaciones críticas, será el resultado del análisis de impacto realizado por el Responsable de Seguridad Informática conjuntamente con los Propietarios de la Información con incumbencia. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.
- Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Deberá realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa.

Dicho análisis será realizado por el Responsable de Seguridad Informática conjuntamente con los Propietarios de la Información. Se dispondrá de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

Asimismo, se procurará que los interruptores de emergencia se ubiquen cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se implementará protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

#### **6.4.7.- SEGURIDAD DEL CABLEADO**

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra interceptación o daño, mediante las siguientes acciones:

- Utilizar piso falso o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información. En su defecto estarán sujetas a la siguiente protección alternativa (indicar protección alternativa del cableado)
- Proteger el cableado de red contra interceptación no autorizada o daño mediante controles (ejemplo: el uso de conductos o evitando trayectos que atraviesen áreas públicas).
- Separar los cables de energía de los cables de comunicaciones para evitar interferencias.
- Proteger el tendido del cableado troncal (backbone) mediante la utilización de canales blindados.

Para los sistemas sensibles o críticos (detallar cuáles son), se implementarán los siguientes controles adicionales:

- Instalar conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
- Utilizar rutas o medios de transmisión alternativos.

#### **6.4.8.- MANTENIMIENTO DE EQUIPOS**

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

- Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsables del Área Informática. El Área de Informática mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
- Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- Registrar el retiro de equipamiento de la sede de la organización para su mantenimiento.
- Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

#### **6.4.9.- SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES.**

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito del Organismo, será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Propietario de la misma.

La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la organización para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito de la organización, cuando sea conveniente.

#### **6.4.10.- REUTILIZACIÓN SEGURA DE LOS EQUIPOS.**

La información puede verse comprometida por una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

#### **6.5.- POLÍTICAS DE ESCRITORIOS Y PANTALLAS LIMPIAS.**

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán los siguientes lineamientos:

- Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- Guardar bajo llave la información sensible o crítica de la organización (preferentemente en una caja fuerte a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.
- Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o

copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.

- Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.
- Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.
- Retirar inmediatamente la información sensible o confidencial, una vez impresa.

#### **6.6.- POLITICA DE RETIRO DE LOS BIENES**

El equipamiento, la información y el software no serán retirados de la sede de la organización sin autorización formal.

Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la organización, las que serán llevadas a cabo por el responsable (indicar el Área responsable). El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.

## **CONCLUSIONES GENERALES**

En los tiempos actuales se toca mucho el tema de seguridad de la información, implantación de políticas, certificaciones en seguridad, etc y se argumenta que las empresas deben requerirlas para cumplir con sus requerimientos de seguridad de la información pero la realidad es que son muy pocas las empresas que están conscientes con respecto a este tema. Estas siempre tienen necesidades empresariales que deben desarrollar e implementar pero casi nunca la relacionan con seguridades.

Una Política de Seguridad de la Información generalmente exige que todos en la organización protejan la información para que la empresa pueda cumplir con sus responsabilidades reglamentarias, jurídicas y fiduciarias. Muchas veces se tiene la idea de que para tener seguridad se debe realizar una gran inversión no solo en dinero sino en tiempo y recursos, por lo que las empresas medianas y pequeñas no lo ven muchas veces justificable o también se tiene la idea errónea de que se deben cumplir al pie de la letra toda la norma o práctica de seguridad escogida para implementar en la empresa. Pero la inversión adicional para proteger la información no siempre garantiza el éxito, pero si es recomendable tener un presupuesto asignado para cumplir con estos fines.

Para evaluar las necesidades de inversión de las empresas, estas deberían responder a las siguientes interrogantes:

- Saber qué información tiene y donde se encuentra.
- Saber el valor de la información que se tiene y la dificultad de volverla a crear si se daña o pierde.
- Saber quiénes están autorizados para acceder a la información y que pueden hacer con ella.
- Saber la velocidad con que puede acceder a la información si no está disponible por alguna razón ya sea por pérdida, modificación no autorizada, etc.

Estas interrogantes son aparentemente simples. Sin embargo, las respuestas permitirán el diseño e implementación de un programa de protección a la información puesto que las respuestas pueden ser muy difíciles. No toda la información tiene el mismo valor y por lo tanto no requiere el mismo nivel de protección tomando en cuenta el costo que implica.

Por lo tanto es clave entender por qué se necesita proteger la información y así determinar la necesidad de tener una Política de Seguridad de la Información. Para ello, se necesitara saber cuál es la información y en donde se encuentra para que pueda proceder a definir los controles que se necesitan para protegerla.

Pero no es simplemente ver que tiene de malo o bueno con respecto a la tecnología que poseen o como se llevan las cosas en el departamento de sistemas, va mucho mas allá, es comprender el negocio, su misión y visión, conocer sus objetivos para de acuerdo a esto diseñar un plan de sistema de gestión de seguridad de la información que vaya alineado a lo que la Institución realmente necesita de acuerdo a sus objetivos.

El Hospital Universitario a pesar del poco tiempo que tiene se ha preocupado por buscar una guía para implementar seguridades y control en el manejo de la información.

Después que se logro realizar el respectivo análisis de riesgo y su impacto en el negocio nos dio como resultado que la Institución tiene muchas vulnerabilidades y puede ser muy afectada si se llegara a materializar los riesgos que tienen y que esto se da por el desconocimiento o no concientización del personal con respecto a la seguridad de la información aparte que no tienen bueno diseños de controles por lo tanto son no efectivos y los controles que tienen y que están bien diseñados muchas veces no se cumple con el procedimiento.

En base a esto se procede a diseñar un plan de sistema de gestión de seguridad de la información basada en una metodología en nuestro caso COBIT que es un modelo de buenas prácticas reconocida y aceptada internacionalmente para el manejo de seguridades y control de la información. Se llevo a cabo la creación de políticas de seguridad que deben ser publicadas o promocionadas para todo el personal ya que es



la base para llevar con éxito la implementación de un sistema de gestión de seguridad de la información.

Estas políticas de seguridad poseen características principales como son:

- Que están escritas en lenguaje simple para una fácil comprensión.
- están basadas en las razones que tiene la empresa para proteger la información.
- Debe ser consistente con las demás políticas organizacionales.
- Que toma en cuenta los aportes hechos por las personas afectadas por la política.
- Que se definen roles y responsabilidades de los usuarios y departamentos para los que aplica la política.
- No debe violar las políticas locales, estatales.
- Se definen las consecuencias en caso de incumplimiento de la política.
- Que debe estar respaldada por documentos palpables, como son los estándares y procedimientos para la seguridad de la información.
- Que estas se adapten a los cambios en las operaciones de las empresas, las necesidades, los requerimientos jurídicos y los cambios tecnológicos.

Debe ser aprobada y firmada por el gerente general de la Institución ya que al no obtener este compromiso significa que el cumplimiento de la política es opcional, situación que hará que fracase las políticas de protección de la información.

## GLOSARIO

### A

**Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

**Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

### B

**Bases de Datos:** Es un conjunto de datos interrelacionados y un conjunto de programas para accederlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápida.

### C

**COBIT :** (Control Objectives for Information and Related Technology); metodología desarrollada como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información.

**Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

**Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

**Control Interno:** las políticas, procedimientos, prácticas y estructuras organizativas diseñadas para proveer una garantía razonable de que se pueden lograr los objetivos y de que se impedirán o detectarán y corregirán los casos no deseados.

**Controles correctivos:** son diseñados para corregir los errores, las omisiones y los usos e intrusiones no autorizados una vez que estos sean detectados.

**Control de Detección:** sirven para detectar y para reportar cuando ocurran errores, omisiones y el uso o el ingreso no autorizado

**Controles Preventivos:** estos controles están diseñados para impedir o para restringir un error, omisión o una intrusión no autorizada.

## D

**Declaración de aplicabilidad:** documento que describe los objetivos de control y los controles pertinentes y aplicables para un sistema de gestión de la información de la organización, con base en los resultados y conclusiones de los procesos de valoración y tratamiento e riesgos.

**Disponibilidad:** Seguridad de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando los requieran.

## E

**Evaluación del riesgo:** evaluación de amenazas a la información, impactos sobre esta y vulnerabilidades de ella y de los medios usados para su procesamiento y de su probable ocurrencia.

**Exposición:** un resultado o consecuencia potencialmente adversa a ser considerada al evaluar los controles internos. Fortalecer los controles internos puede reducir la exposición pero rara vez la elimina.

## G

**Gestión del riesgo:** proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que puedan afectar a los sistemas de información.

## I

**Integridad:** protección de la exactitud y estado completo de la información y métodos de procesamiento.

**Irregularidades:** violaciones intencionales de la política establecida o declaraciones falsas intencionales u omisiones de información.

## N

**No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

## O

**Objetividad:** capacidad del auditor de sistemas de información para ejercer su juicio, expresar opiniones y presentar recomendaciones con imparcialidad.

**Objetivo de seguridad:** es la declaración expresa de la intención de conseguir algo que contribuye a la seguridad de la información, bien porque se opone a una de las amenazas identificadas o bien porque satisface una exigencia de la política de seguridad de la información.

## P

**Principio:** es una norma o idea fundamental que rige la Política de Seguridad, y que se acepta en esencia.

**Privacidad:** involucra proveer la protección debida a la información identificable y personal relacionada con un individuo identificado o identificable(sujeto de datos)

**Política de seguridad de la información:** como el conjunto de normas, reglas, procedimientos y prácticas que regulan la protección de la información contra la pérdida de confidencialidad, integridad o disponibilidad, tanto de forma accidental como intencionada.

**Posibles consecuencias:** Corresponde a los posibles efectos ocasionados por el riesgo, los cuales se pueden traducir en daños de tipo económico, social, administrativo, entre otros

**Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

## R

**Riesgo:** El potencial de que una amenaza determinada explote las vulnerabilidades de un activo y que ocasione perdida y daño de los mismos. Usualmente se mide mediante la combinación del impacto y e la probabilidad que ocurra.

**Riesgo residual:** nivel restante de riesgo después que se han tomado medidas de tratamiento del riesgo.

Riesgo de Control: el riesgo de que haya un error material que no fuera prevenido ni detectado oportunamente por el sistema de controles internos.

## S

**Seguridad de la Información:** preservación de la confidencialidad, la integridad y la disponibilidad de la información

**Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

**Sistema de Gestión de seguridad de la información:** parte del sistema de gestión global, basada en un enfoque hacia los riesgos de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información

## T

**Tecnología de la Información:** Se refiere al hardware y software operados por la Institución

o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

**Tratamiento el riesgo:** proceso de selección e implementación de medidas para tratar el riesgo

## V

**Valoración del riesgo:** proceso global de análisis y evaluación del riesgo.

## BIBLIOGRAFÍA

- COBIT 3ra Edición
- COBIT <http://www.isaca.org/cobit>
- Norma ISO 17799
- <http://www.palermo.edu.ar/cyt/pdf/COBIT.pdf>
- [www.bsiamericas.com/seguridaddelainformacion](http://www.bsiamericas.com/seguridaddelainformacion)
- <http://www.infosecuritymag.com/2002/nov/nightmares.shtml>
- Auditoría de Sistemas y Seguridades  
<http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/index.html>
- ¿Como elaborar políticas de Seguridad efectivas?  
<http://www.symantec.com/region/mx/enterprisesecurity>
- Gestión Integral del Riesgo  
<http://www.pc-news.com/detalle.asp?sid=&id=11&Ida=2188>
- Gestión de Contraseñas <http://www.securityfocus.com/infocus/1537>
- Evaluación de Seguridad de un Sistema de Información  
<http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml#top>

## **ANEXO A:**

### **SITUACION ACTUAL DE LA EMPRESA**

Esto fue tomado en base a una auditoria anterior que se realizo como proyecto .

### **INTRODUCCIÓN**

El Sistema Hospitalario Docente de la Universidad de Guayaquil, es un Centro Hospitalario de cuarto nivel, con proyección a brindar servicios de investigación científica, relativamente nuevo, abrió sus puertas para atención al público en el mes de abril, actualmente cuenta con servicios de consulta externa en el área ginecológica, consulta externa general además de servicios de apoyo como son Laboratorio, Imágenes y Odontología

### **MOTIVOS PARA LA REALIZACIÓN DE LA AUDITORÍA.**

La auditoria de los sistemas que manejan la información surge como un primer paso en la consecución de un gran objetivo crear un PLAN PARA LA GESTION DE SEGURIDAD DE LA INFORMACIÓN.

Conociendo la apertura que hemos tenido por parte de las Autoridades de la Universidad y en especial del Hospital, estos se comprometieron a entregar la información requerida y a brindar las facilidades necesarias para realizar el trabajo.

### **OBJETIVOS**

- Verificar la existencia de controles dentro del área de PED:
  - Seguridades Físicas
  - Seguridades de Mantenimiento.
  - Seguridades Lógicas
  - Seguridades de Datos
  - Seguridades de Red, Telecomunicaciones, SO.
  - Procedimientos para Desarrollo de Sistemas.
  - Procedimientos para el Mantenimiento de Hardware y Software.



- Procedimientos de Soporte a usuarios.
- Verificar el cumplimiento de las normativas que son resultado de los controles.
- Sugerir nuevos controles para el área de PED si fueren necesarios.
- Verificar la existencia de manuales de procedimiento y funciones en el área de PED.
- Verificar que los trabajos se realicen tomando en cuenta las indicaciones de dichos manuales.
- Analizar el uso de los recursos informáticos.

## **ALCANCE**

El trabajo de Auditoria focaliza sus actividades sobre el Departamento de Sistemas y en la información que este maneja. Dicho trabajo contempla:

Verificar, definir y dar sugerencias tendientes a solucionar problemas encontrados por el grupo de auditoria en el transcurso del desarrollo del trabajo. Así como problemas concernientes a:

Evaluación de equipos en:

- Seguridades Físicas
- Procedimientos de Adquisición de Hardware y Software.
- Manuales

Evaluación de los sistemas en:

- Seguridades de Datos.
- Seguridades de mantenimiento.
- Respaldos
- Manuales
- Estándares de Desarrollo de Aplicaciones.

Se evaluará también:

- Seguridades en Redes y Telecomunicaciones.
- Seguridades de Sistemas Operativos.
- Estructura Orgánica-Funcional del Centro de Cómputo.
- Funciones del personal.
- Manuales de Funciones y Procedimientos
- Capacitación del Personal.
- Procedimientos de Soporte a usuario.
- Elaboración de los informes que contengan conclusiones y recomendaciones.

Cabe recalcar que el trabajo de auditoria se desarrolla dentro del centro de cómputo. Además no estarán involucrados en dicho trabajo ninguno de los otros departamentos de la institución.

## **AREAS DE ACCIÓN**

El trabajo del grupo de Auditoría se centrará en las siguientes áreas de acción:

- Librerías de manuales
- Bitácoras
- Suministros
- Instalaciones
- Plataforma Operativa
- Distribución de la Red.

## **RECURSOS**

El trabajo de auditoría a realizar necesitará de la utilización de los siguientes recursos:

- Recursos humanos:
  - Auditor Supervisor.  
Ing. Luis Dier Luque (1)
  - Auditores de apoyo tipo senior. (2)  
Ing. Angélica Aguiar Ayala.  
Ing. Sisiana Chávez Chica.
- Equipos y Materiales:

El hardware y software requerido para le ejecución de la auditoria, además del papel, útiles de oficina y otros materiales serán proporcionados por el grupo de auditores.
- Financieros:

Todo lo necesario para cubrir la auditoria será proporcionado por el grupo de auditores.

## INFORMACIÓN GENERAL DE LA EMPRESA

EMPRESA: Sistema Hospitalario Docente de la Universidad de Guayaquil

MISIÓN DE LA EMPRESA: La misión de la Empresa es brindar servicios y atención médica de calidad, así como formar médicos con suficiente capacidad de análisis e investigación que fomenten en el país la conciencia de ayuda social.

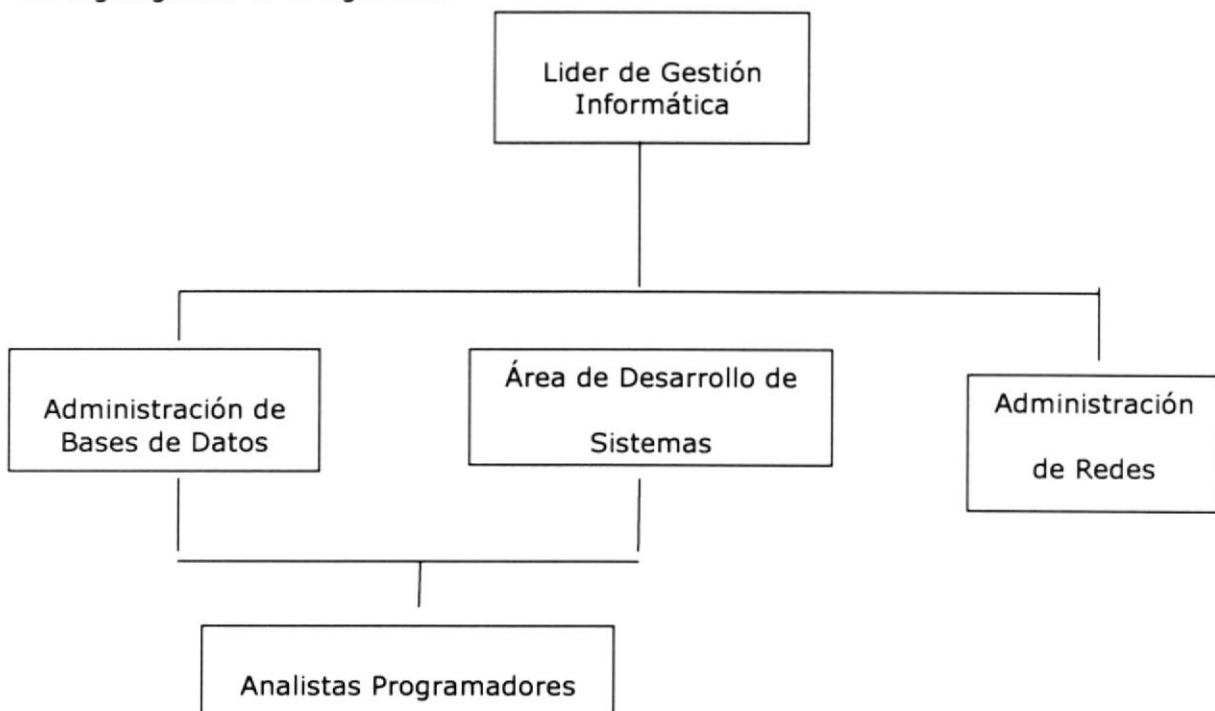
## DISTRIBUCIÓN ORGANIZACIONAL DE LA EMPRESA

La Empresa cuenta con su sede principal en la ciudad de Guayaquil, su Directora General es la Dra. Manuelita Yuen Chon, se encuentran aperturadas las unidad de Ginecología y Odontología, así como los servicios de apoyo de laboratorio, imágenes y patología.

Cada unidad tiene su Director, en la Unidad Ginecológica, donde se encuentran los servicios de apoyo, también se encuentra ubicado el Departamento de Sistemas, ubicación que es provisional, puesto que su ubicación final será el Edificio de Docencia.

## ESTRUCTURA ORGÁNICO FUNCIONAL DEL DEPARTAMENTO DE SISTEMAS.

Su organigrama es el siguiente:



## **FUNCIONES DEL PERSONAL DEL DEPARTAMENTO DE SISTEMAS**

**Cargo:** Líder de Gestión Informática.

**Responsabilidades:** Reporta al Director General.

Entre sus funciones básicas está el dirigir la ejecución de los distintos proyectos que se realicen, Guiar en la elaboración de manuales técnicos y asesoría a los usuarios en el uso de las aplicaciones y utilitarios.

### **FUNCIÓN**

1. Realizar estudios de automatización en las diversas áreas de la empresa, de acuerdo a un plan maestro de sistemas.
2. Analizar los procesos manuales y mecánicos que se llevan a cabo actualmente y reemplazarlos con aplicaciones automatizadas.
3. Supervisar el respaldo de programas ejecutables y fuentes, los mismos que serán entregados al director de sistemas.
4. Elaborar manuales de operación de las aplicaciones desarrolladas.
5. Capacitar al personal involucrado en la implementación de un nuevo sistema.
6. Decidirá la acción a tomar en cualquier eventualidad de falla en el computador central o en el proceso de respaldo.
7. Asesoría al usuario final en el mejor uso de alguna aplicación o utilitario orientándolo hacia la eficiencia en su operación.
8. Presentará un informe mensual de las principales incidencias sucedidas en el respectivo mes.

**Cargo:** Analista Programador.

**Responsabilidades:** Reporta al Jefe de Sistemas.

Realizar tareas de análisis, desarrollo y programación de aplicaciones. Elaborar manuales técnicos y asesoría a los usuarios en el uso de las aplicaciones y utilitarios.

## **FUNCIÓN**

1. Realizar estudios de automatización en las diversas áreas de la empresa, de acuerdo al plan maestro de sistemas.
2. Presentará un informe mensual de las principales incidencias sucedidas en el respectivo mes.
3. Analizar los procesos manuales y mecánicos que se llevan a cabo actualmente y reemplazarlos con aplicaciones automatizadas.
4. Programar en el lenguaje establecido, las aplicaciones anteriormente estudiadas.
5. Elaborar manuales de operación de las aplicaciones desarrolladas.
6. Capacitar al personal involucrado en la implementación de un nuevo sistema.
7. En coordinación con el director de sistemas, elaborar un cronograma de actividades.
8. Decidirá la acción a tomar en cualquier eventualidad de falla en el computador central o en el proceso de respaldo.
9. Asesorar al usuario final en el mejor uso de alguna aplicación o utilitario orientándolo hacia la eficiencia en su operación.
10. Tendrá reuniones quincenales con el jefe de sistemas para analizar el avance y ejecución del cronograma de actividades.

### **Cargo: Administrador de Red.**

**Responsabilidades:** Reporta al Jefe de Sistemas.

Administrar la red de Pc en las redacciones, producción y publicidad, supervisar diariamente el funcionamiento y estado del equipo de computación de las redacciones y producción así como el sistema computarizado de biblioteca y de comunicación con esa gráfica, asistir y entrenar a usuarios de estos equipos.

## **FUNCIÓN**

1. Revisará los equipos de la red, para que estén aptos para el uso de redactores y usuarios en Quito y Guayaquil.



## **SISTEMAS EXISTENTES**

✓ SHDUG Este software ha sido desarrollado internamente.

Consta de los módulos:

- Ginecología
- Pediatría
- Laboratorio
- Imágenes
- Citología
- Admisión
- Información
- Caja

### **• Generalidades Software**

- La Base de Datos que el Hospital maneja es SQL Server 2000 en un servidor HP, con Sistema Operativo Windows 2003 Server, las licencias las provee la Universidad de Guayaquil mediante el convenio Campus Agreement.
- El sistema existente esta hecho en Visual Basic .net
- En cuestión de seguridades se manejan en base a perfiles de cada usuario. Es decir, tienen un perfil por cada grupo de usuarios.
- Existen seguridades a nivel menús y programas, todo en base a permisos de acceso otorgados a los usuarios. Además de aquello también se tienen controles a nivel de programa sobre el tipo de acción que puede tener determinado usuario con la información que maneja (Permiso de solo lectura, escritura, modificación, eliminación en la base de datos)
- El Sistema es un conjunto de módulos que son invocados desde uno principal llamado pryShdug, estos módulos interactúan e intercambian información entre ellos. Estos sistemas tienen 6 meses funcionando.

- Dichos sistemas funciona aceptablemente, el departamento de sistemas de la institución se encarga de realizarle mejoras y/o adecuaciones y/o actualizaciones en base a requerimientos que se dan por circunstancias internas de la empresa o situaciones externas.

### **Recopilación de Información**

Empleados Entrevistados:

Lider de Gestión Informática

Administrador de Base de Datos

Jefe Área de Desarrollo

7 Analistas –Programadores. (pasantes)

### **EXAMEN DETALLADO DE LAS ÁREAS CRITICAS**

#### **• DETALLE DE FALTAS DE CONTROL EN LA ORGANIZACIÓN DEL AREA DE PED**

Problema:	No existe definido un manual de funciones para el personal del Departamento de Sistemas.
Efecto:	Que las labores que realicen este personal no sean las adecuadas para el cargo, no sean suficientes y causen confusión.
Recomendación:	Definir funciones para el personal del departamento de sistemas y elaborar un manual que contenga las funciones versus perfil del cargo.

Problema:	Existen deficiencias en el control y cumplimiento a tiempo de los trabajos encomendados.
Efecto:	Cuando se acerca la entrega de avances, existe bastante presión. Esto se repite por varios días seguidos, ocasionando que el recurso humano disponible se agote, se distorsionen los horarios de trabajo y se pierda el ritmo laboral.
Recomendación:	Realizar un control periódico de los progresos en los trabajos encomendados, utilizar un tiempo de jornada laboral diaria adecuado para avanzar en las asignaciones pero sin agotar al



	recurso humano.
--	-----------------

Problema:	No existen Planes de Contingencia para ningún tipo de adversidad que se pudiera presentar.
Efecto:	No se conoce la forma de proceder si ocurre alguna emergencia
Recomendación:	Elaborar planes de contingencia con respecto a todos los riesgos que se suponen pueden ocurrir. Realizar simulacros con respecto a lo especificado en el plan.

• **FALENCIAS EN LAS SEGURIDADES DE DATOS**

Problema:	No existen planes de emergencia con respecto a la seguridad de datos.
Efecto:	No se conoce la forma de proceder si ocurre alguna emergencia en los datos
Recomendación:	Elaborar planes de contingencia con respecto a todos los riesgos que se suponen pueden ocurrir. Realizar simulacros con respecto a lo especificado en el plan.

Problema:	No existen documentación, procedimientos escritos con instrucciones concretas acerca del uso de los programas y aplicaciones.
Efecto:	Las personas que manejan dichos programas o aplicaciones pueden tornarse imprescindibles y nadie podría reemplazarlas en un momento determinado, cuestión que va en detrimento de la seguridad de la empresa. Puede existir corrupción de los datos al ingresarlos a los aplicativos o programas si no se lo hace siguiendo un procedimiento.
Recomendación:	Elaborar un manual de procedimientos para el uso de aplicativos y programas.

• **FALENCIAS EN LAS SEGURIDADES FÍSICAS**

Problema:	Los empleados que van a laborar a la empresa fuera del horario normal de trabajo, el Jefe del Departamento envía un oficio al
-----------	---

	SAF indicando las personas que van a entrar y que se disponga el transporte necesario, no se comunican horas de entrada y salida, no se controla quien de esas personas pueden entrar al centro de cómputo ya que no existe una vigilancia a la entrada del Centro de Cómputo.
Efecto:	Personal no autorizado puede acceder al área de Ped lo que podría causar inconvenientes pues se trata de un área neurálgica para la institución.
Recomendación:	Prohibir el ingreso y controlar estrictamente al personal que tiene acceso al área de Ped.

Problema:	Existen alarmas para detección de incendios, pero no se ha comprobado su funcionamiento
Efecto:	No existe al momento, forma de comprobar si estos dispositivos funcionan.
Recomendación:	Comprobar que dichos dispositivos de detección en el centro de cómputo funcionen, realizar simulacros.

Problema:	No existen extintores de incendios en el Departamento de Sistemas.
Efecto:	En caso de ocurrir algún conato de incendio no podría eliminárselo con la respectiva prontitud y los daños podrían ser mayores.
Recomendación:	Instalar en el centro de cómputo algún sistema de control de incendios, preferiblemente con materiales que no comprometan la vida de las personas ni la integridad de los equipos.

Problema:	No existen manuales o reglamentos para la seguridad física del Centro de Cómputo.
Efecto:	Las personas no conocen las reglas ni las precauciones que tienen que tomar al hacer alguna actividad específica o al encontrarse en el área de PED.
Recomendación:	Elaborar manuales y reglamentos. Controlar el cumplimiento de las normas ahí establecidas

Problema:	Cerca del Centro de cómputo existen servicios comunitarios como son los baños.
Efecto:	Personas no autorizadas podrían acceder al centro de cómputo debido al tránsito de diversas personas por el lugar.
Recomendación:	Ubicar el baño en otro lado o en su defecto trasladar al centro de cómputo hacia un lugar mas adecuado.

• **FALENCIAS EN EL DESARROLLO DE APLICACIONES**

Problema:	No se tiene un control adecuado de las versiones de programas y aplicativos.
Efecto:	Confusiones pueden generarse al momento de enviar un aplicativo a producción y de ocurrir un error no existe la posibilidad de arreglarlo inmediatamente por que los cambios no son documentados.
Recomendación:	Documentar todos los cambios que se realicen. Realizar un estricto control de las versiones de los aplicativos utilizando la documentación respectiva.

Problema:	No existen manuales de los programas.
Efecto:	Si alguna persona quiere realizar la utilización de algún programa o aplicativo tiene que recurrir necesariamente al personal de soporte lo que provoca demoras en el trabajo.
Recomendación:	Elaborar manuales del usuario para cada aplicativo que se lleva a producción.

Problema:	El DBA además de estar a cargo de la supervisión del desempeño de actividades, también programa.
Efecto:	El jefe de Sistemas debe dedicar gran parte de su tiempo a tareas que no son parte de su perfil, y esto hace que se descuiden asuntos importantes de la administración del centro de cómputo.
Recomendación:	Redefinición de las funciones del cargo de acuerdo al perfil.

Problema:	Se dan cuellos de botella en el proceso de desarrollo de Software.
Efecto:	Se producen los denominados cuellos de botella que atrasan el desarrollo de software.
Recomendación:	Establecer una política de gestión de requerimientos, con la que todos los miembros de la organización se encuentren comprometidos, para de esta manera verificar los requerimientos primordiales para darles trámite inmediato.

• **FALENCIAS EN LA SEGURIDAD DE MANTENIMIENTO**

Problema:	Los equipos no tienen cobertores ni ningún tipo de material de protección.
Efecto:	Disminución del tiempo de vida de los equipos.
Recomendación:	Adquirir cobertores para los equipos y realizar limpiezas mas frecuentes a los mismos.

Problema:	No existen procedimientos de operación escritos para encender y apagar el computador en operaciones anormales
Descripción:	Si ocurre alguna falla en los sistemas (inhibiciones) no existen procedimientos a seguir con respecto al apagado o encendido del computador.
Efecto:	El computador puede sufrir daños por manejo inadecuado del apagado o el encendido.
Recomendación:	Brindar documentación indicando pasos a seguir en dichos casos.

Problema:	Los servidores quedan todo el tiempo encendidos y no todos utilizan protector de pantalla.
Descripción:	El servidor Windows 2003 usa protector de pantalla con clave,
Efecto:	Disminución del tiempo de vida de los equipos ya que son

	expuesto a dañarse ya que pueden sobrecalentarse. Además cualquier persona no autorizada que logre entrar al área de Pad podría borrar o modificar las configuraciones de red, cambiar claves, eliminar archivos, etc.
Recomendación:	Se recomienda que mientras no se estén utilizando los servidores se usen protectores de pantallas, con claves.

• **FALENCIAS EN EL SISTEMA OPERATIVO**

Problema:	No hay un registro de las diferentes versiones del Sistema Operativo.
Efecto:	No se puede determinar cual es la mejoría que se ha obtenido al utilizar esa nueva versión del sistema operativo.
Recomendación:	Realizar un registro con los diferentes sistemas operativos que la empresa a utilizado para poder determinar si el cambio de versión fue oportuno o no.

Problema:	No se tiene respaldo de la clave de Administrador en un lugar seguro.
Efecto:	Si por algún motivo es necesario prescindir de los servicios del administrador la persona que venga a ocupar su lugar no va a saber como poder acceder a ciertos lugares en el sistema, que solo el administrador tiene permiso.
Recomendación:	Tener un respaldo de la clave del administrador en un sobre lacrado y en un lugar seguro en la cual solo la persona autorizada tenga acceso.

• **LIBRERÍAS DE MANUALES**

Problema:	No existen manuales de procedimientos, funciones, técnico-operativo de los equipos y sistemas.
-----------	--

Efecto:	Se pueden cometer faltas graves con merecimiento a sanción ocasionadas por el desconocimiento de los procedimientos a seguir para desarrollar una actividad.
Recomendación:	Elaborar e Imprimir un manual de procedimientos , funciones, técnico – operativo de los equipos y sistemas.

• **BITÁCORAS**

Problema:	No se manejan bitácoras de ingreso al Centro de Cómputo tanto para el personal de la empresa como para los visitantes.
Efecto:	No se sabe con exactitud cuantas personas han ingresado durante el día , para que asunto y en el caso de que ocurra un problema no se sabe quien es el responsable.
Recomendación:	Poner una persona responsable de llenar una bitácora de ingreso del personal con su nombre completo, la hora de ingreso, asunto por el que vino y la hora de salida del centro de cómputo.

Problema:	No se prestan, ni se adquieren manuales, los manuales que vienen con los software, ellos no lo utilizan porque consideran que tienen lo básico y no les sirve.
Efecto:	Que no tengan conocimiento de lo último de la tecnología, recordar detalles que a pesar de ser básicos son importantes y uno los puede olvidar.
Recomendación:	Adquirir manuales de algún software específico, elaborar manuales de los sistemas, y llevar un registro de entrada/salida del software y de los manuales respectivos.

• **INSTALACIONES**

Problema:	No hay un control estricto de procedimientos en el servicio de seguridad de la empresa.
Efecto:	Personas que quisieran realizar un sabotaje, robo o alterar

	información no tendrán ningún obstáculo difícil de pasar para poder acceder al Centro de Computo.
Recomendación:	Se debería bloquear todo tipo de acceso no permitido al centro de cómputo.

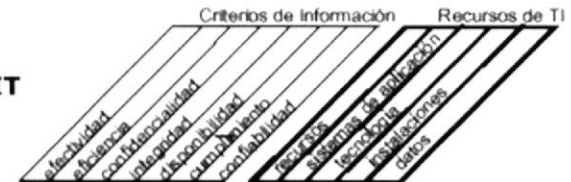
• **PLATAFORMA OPERATIVA**

Problema:	No existen manual de políticas para la administración de base de datos
Efecto:	Se dificulta la capacitación de los operadores. En ocasiones los operadores deben realizar las tareas del administrador de la base de datos y no tienen sobre qué guiarse en su ausencia o para una simple consulta.
Recomendación:	Se recomienda elaborar un manual de este tipo que explique de una manera concisa las operaciones básicas y comunes que se realicen sobre la base de datos y deben estar al alcance del operador.

Problema:	No existe manual de levantamiento de la base de datos
Efecto:	En casos de emergencia, la ausencia del administrador de la base de datos provocaría la interrupción de las actividades de la empresa.
Recomendación:	Se recomienda definir por escrito los pasos necesarios.

**ANEXO B**

**SELECCIÓN DE PROCESOS Y OBJETIVOS DE CONTROL BASADOS EN EL MODELO COBIT**



DOMINIO	PROCESO	Criterios de Información							Recursos de TI					
		efectividad	eficiencia	confiabilidad	integridad	disponibilidad	cumplimiento	confidencialidad	recursos	sistemas de información	tecnologías	instalaciones	datos	
Planeación y Organización	PO1	Definir un plan estratégico de sistemas	P	S					X	X	X	X	X	
	PO2	Definir la arquitectura de información	P	S	S	S				X			X	
	PO3	Determinar la dirección tecnológica	P	S							X	X		
	PO4	Definir la organización y sus relaciones	P	S						X				
	PO5	Administrar las inversiones (en TI)	P	P				S		X	X	X	X	
	PO6	Comunicar la dirección y objetivos de la gerencia	P					S		X				
	PO7	Administrar los recursos humanos	P	P						X				
	PO8	Asegurar el apego a disposiciones externas	P					P	S	X	X		X	
	PO9	Evaluar riesgos	S	S	P	P	P	S	S	X	X	X	X	X
	PO10	Administrar proyectos	P	P						X	X	X	X	
	PO11	Administrar calidad	P	P		P		S		X	X			
Adquisición e Implementación	AI1	Identificar soluciones de automatización	P	S						X	X	X		
	AI2	Adquirir y mantener software de aplicación	P	P		S	S	S		X				
	AI3	Adquirir y mantener la arquitectura tecnológica	P	P		S					X			
	AI4	Desarrollar y mantener procedimientos	P	P		S	S	S		X	X	X	X	
	AI5	Instalar y acreditar sistemas de información	P			S	S			X	X	X	X	X
	AI6	Administrar cambios	P	P		P	P	S		X	X	X	X	X
Entrega de servicios	DS1	Definir niveles de servicio	P	P	S	S	S	S	S	X	X	X	X	X
	DS2	Administrar servicios de terceros	P	P	S	S	S	S	S	X	X	X	X	X
	DS3	Administrar desempeño y capacidad	P	P			S				X	X	X	
	DS4	Asegurar continuidad de servicio	P	S				P		X	X	X	X	X
	DS5	Garantizar la seguridad de sistemas			P	P	S	S	S	X	X	X	X	X
	DS6	Identificar y asignar costos		P					P	X	X	X	X	X
	DS7	Educar y capacitar a usuarios	P	S						X				
	DS8	Apoyar y orientar a clientes	P							X	X			
	DS9	Administrar la configuración	P				S	S		X	X	X		
	DS10	Administrar problemas e incidentes	P	P			S			X	X	X	X	X
	DS11	Administrar la información				P			P					X
	DS12	Administrar las instalaciones					P	P					X	
	DS13	Administrar la operación	P	P		S	S			X	X		X	X
Monitoreo	M1	Monitorear el proceso	P	S	S	S	S	S	S	X	X	X	X	X
	M2	Evaluar lo adecuado del control interno	P	P	S	S	S	S	S	X	X	X	X	X
	M3	Obtener aseguramiento independiente	P	P	S	S	S	S	S	X	X	X	X	X
	M4	Proporcionar auditoría independiente	P	P	S	S	S	S	S	X	X	X	X	X



*Rueda Indebida 11420201*

tipo	detalle	vencido	por_vencer	total	peso	cabecera	localidad	saldo_contable
1	Autoservicios	3046.69	2320.05	5,366.74		CUENTA	11410101	0
1	→ Empresas Relacionar	9583.61	66492.53	76,076.14		CUENTA	11410101	0
1	Supermercados	-2365.39	192391.55	190,026.16		CUENTA	11410101	0
	<b>Total 11410101</b>			<b>271,469.04</b>				<b>195,392.90 le resto Empresas Relacionadas</b>
1	Clientes Especiales	-19490.33	3333.23	-16,157.10		CUENTA	11410102	0
1	Detallistas	-142	0	-142.00		CUENTA	11410102	0
1	Empleados	0	139.77	139.77		CUENTA	11410102	0
1	Empresas	1708.16	913.52	2,621.68		CUENTA	11410102	0
1	Estaciones de Servic	538.7	1680.53	2,319.23		CUENTA	11410102	0
1	Farmacias	643.53	7828.92	8,472.45		CUENTA	11410102	0
1	Fast Food	26.64	7400.29	7,426.93		CUENTA	11410102	0
1	Inst. FF. AA.	6457.6	3723.5	10,181.10		CUENTA	11410102	0
1	Moteles/Hoteles	80.68	658.14	738.82		CUENTA	11410102	0
1	Otros	10.65	178.6	189.25		CUENTA	11410102	0
1	Panaderias	247.94	395.83	643.77		CUENTA	11410102	0
1	Restaurants/Cafeteri	267.13	466.44	733.57		CUENTA	11410102	0
1	Vendedores de Ciuda	0	-5.52	-5.52		CUENTA	11410102	0
1	Vendedores de Pan c	24.99	0	24.99		CUENTA	11410102	0
	<b>Total 11410102</b>			<b>17,186.94</b>				<b>92,888.68 le sumo Empresas relacionadas menos inalecsa 374.40</b>
1	Vendedores de Provi	0	0	0.00		CUENTA	11410103	0
	<b>Total 11410103</b>			<b>0.00</b>				
1	Distribuidoras de Ciu	-2,8422E-14	0	0.00		CUENTA	11410104	0
	<b>Total 11410104</b>			<b>0.00</b>				
1	Distribuidores de Pro	19007.69	64903.17	83,910.86		CUENTA	11410105	0
	<b>Total 11410105</b>			<b>83,910.86</b>				<b>83,910.86</b>
1	Exportacion	-995.39	18725.94	17,730.55		CUENTA	11410107	0
	<b>Total 11410107</b>			<b>17,730.55</b>				<b>17,730.55</b>
	<b>Total 11420201</b>			<b>390,297.39</b>				<b>374.4</b>
	<b>Total general</b>			<b>390,297.39</b>				<b>390297.39</b>