CONTENIDO

ANEXOS

1. OBJETIVO

El objetivo de nuestra tesis es el Diseño de un Sistema de Gestión de Seguridad de la Información para la empresa ECUACOLOR, basado en el análisis de la empresa y el conocimiento adquirido durante el Diplomado de Auditoría Informática

Un segundo objetivo es contribuir para que las empresas ecuatorianas tomen conciencia de la necesidad de implementar Sistemas de Seguridad, como una herramienta que ayudará a cumplir con las metas y objetivos de la empresas, ayudándoles en la gestión del negocio y ser más competitivas en el mercado.

2. INTRODUCCIÓN

A finales del siglo XX, los Sistemas Informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, “Los Sistemas de Información” de la empresa.

La Informática hoy, es la base en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a controles. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, se hace necesario un Sistema de Gestión de Seguridad de Información.

La información en la empresa es uno de los mas importantes activos que posee. Las organizaciones tienen que desarrollar mecanismos que les permitan asegurar la disponibilidad, integridad y confidencialidad en el manejo de la información. La información está sujeta a muchas amenazas tanto de índole externa como externa.

Por eso, al igual que los demás órganos de la empresa (Balances y Cuentas de Resultados, Tarifas, Sueldos, etc.), los Sistemas Informáticos están sometidos al control correspondiente, o al menos debería estarlo.

La importancia de llevar un control de los recursos de los Sistemas de Tecnología de Información se puede deducir de varios aspectos. He aquí algunos:

- Las computadoras y los Centros de Proceso de Datos se convirtieron en blancos apetecibles no solo para el espionaje, sino para la delincuencia y el terrorismo.
- Los hackers que son expertos en Ingeniería Social – consiguiendo personas de dentro de la compañía para sacarles contraseñas y claves de invitados.
- Las computadoras creadas para procesar y difundir resultados o información elaborada pueden producir resultados o información errónea si dichos datos son, a su vez, erróneos. Este concepto obvio es a veces olvidado por las mismas empresas que terminan perdiendo de vista la naturaleza y calidad de los datos de entrada a sus Sistemas Informáticos, con la posibilidad de que se provoque un efecto cascada y afecte a Aplicaciones independientes.
- Un Sistema Informático mal diseñado puede convertirse en una herramienta harto peligrosa para la empresa: como las maquinas obedecen ciegamente a las órdenes recibidas y la modelización de la empresa está determinada por las computadoras que materializan los Sistemas de Información, la gestión y la organización de la empresa no puede depender de un Software y Hardware mal diseñados.

Estos son solo algunos de los varios inconvenientes que puede presentar un Sistema Informático, por eso, la necesidad de un Sistema de Gestión de Seguridad de Información..

Nuestro Proyecto de Diseño de un Sistema de Gestión de seguridad de Información – SGSI – incluye 9 capítulos y 8 anexos.

El capítulo 1, define el objetivo de nuestra tesis, "El diseño de un sistema de Gestión de Seguridad de Información para la empresa ECUACOLOR".

El capítulo 2, es una Introducción sobre la necesidad de implementar en las empresas un SGSI, para el control y protección de los recursos de Tecnología de Información.

El capítulo 3, es el levantamiento de información para el Entendimiento del Negocio, el Marco Operativo y la Tecnología de Información que utiliza ECUACOLOR para el desarrollo de sus operaciones.

El Capítulo 4, es una breve explicación de la herramienta utilizada COBIT, considerada como una de las mejores prácticas para la administración, control, auditoría y manejo de las seguridades de Tecnología de Información.

El capítulo 5, establece la metodología utilizado para el desarrollo de nuestra tesis de graduación.

El capitulo 6, establece el modelo de Madurez de los 7 procesos del modelo COBIT sobre requerimientos de Seguridad (confidencialidad, integridad y disponibilidad), es la situación actual de la empresa y hacía donde quiere llegar.

El capítulo 7, constituye el trabajo de investigación de los 105 objetivos de Control en ECUACOLOR, estableciendo el nivel de riesgo actual (Alto – Medio – Bajo).

El capítulo 8, es el Plan de Acción con los Controles recomendados para la mitigación de los Riesgos cuales.

El capítulo 9, establece los Beneficios que tendría la empresa al implementar un Sistema de Gestión de Seguridad de Información.

Y Finalmente tenemos 8 Anexos, Glosario de términos: Mapa General de Procesos, Organigrama de la Empresa, Organigrama de Sistemas, Proceso de Ventas a Distribuidores y el Proceso de Ventas en Retail.

.

Las Políticas Básica de Seguridad de la Información, que es lo mínimo que debería implementar la empresa.

Como valor agregado hemos incluido los Factores Críticos de Éxito (FCE) y los Indicadores claves de Desempeño , que constituyen herramientas adicionales para llegar a cumplir con éxito la gestión empresarial.

3 ENTENDIMIENTO DEL NEGOCIO

3. 1 INFORMACIÓN INSTITUCIONAL

Reseña Histórica

Laboratorios Fotográficos Ecuacolor es una empresa que nació en la ciudad de Quito hace 35 años gracias a la iniciativa y visión de los señores Luis Orrantia G. y Enrique Martinez Q., Presidente y Gerente General de Comandato de aquel entonces, quienes decidieron crear una empresa dedicada a la venta y procesamiento de las películas en blanco y negro, bajo la razón social de Ecuacolor Laboratorios Fotográficos.

Desde el año 1966, los laboratorios fueron ampliando sus servicios bajo la supervisión de Galo Vinueza, viejo amante de la fotografía y uno de los artífices del desarrollo fotográfico del Ecuador.

En 1975 Ecuacolor ya contaba con un moderno laboratorio de revelado a color en Quito, que fue viendo superada su capacidad de producción por la creciente demanda, por lo que se decidió abrir un nuevo laboratorio. En Marzo de 1976, bajo la supervisión del Ing. Antonio Tobar C., se inauguro uno de los mas modernos laboratorios centrales de Sud América en la ciudad de Guayaquil.

Pocos años después, se inicio a la apertura de punto de revelado satelitales, equipados con mini laboratorios que ofrecían el servicio de revelado en pocas horas. Hoy se cuenta con 106 mini laboratorios instalados en las principales ciudades del país, atendiendo directamente a sus clientes locales, ofreciéndoles productos e innumerables servicios fotográficos y digitales de primerísima calidad.

Ecuacolor se dedica en la actualidad a la captura, reproducción, conservación y comunicación de imágenes que son los mas preciados recuerdos y sentimientos del ser humano.

Gracias a la utilización de tecnología de punta a la experiencia de su recurso humano y a la capacitación continua, ha logrado colocarse como líder en la comercialización y distribución de productos y servicios fotográficos.

Sus mas de 500 colaboradores son el fundamento de la empresa y con orientación total hacia la excelencia que les permite dar un eficiente servicio a todos sus clientes en el país.

MISION

- Lograr la satisfacción de las necesidades de los clientes y usuarios, mediante la entrega de Excelencia en la Calidad de Productos y Servicios dentro de la industria de imágenes.

- Nuestro compromiso con nuestros colaboradores es proveerlos de oportunidades para su desarrollo y crecimiento, remunerándolos mejor que el mercado en base a resultados, e incrementando su patrimonio y bienestar a largo plazo, creando en ellos un recurso valioso.

- Nuestro compromiso con nuestros socios comerciales es el de proveerlos de una plataforma para sus desarrollo sostenido, mediante nuestro crecimiento en ventas y rentabilidad.

- Nuestra responsabilidad con la sociedad y las comunidades en las que operamos , es la de contribuir a su progreso y expectativas para el futuro, y prestar nuestro apoyo para eventos deportivos, culturales y de entretenimiento, que lleven felicidad a sus vidas.

- Entregar a los accionistas el mayor rendimiento a su inversión.

VISION

Ser la empresa de mayor rentabilidad dentro de la industria de imágenes del país, con personal altamente calificado, motivado y profesional; sirviendo en cada área de la empresa y el mercado; con una participación de mercado no menor al 70%.

VALORES

- El cliente es primero.
- Honestidad y lealtad que asegure la integridad de la empresa.
- Capacidad para enfrentar cambios y adaptarnos a nuevas situaciones.
- Educación y aprendizaje constante para lograr la superación personal y profesional.
- Tenacidad y perseverancia para alcanzar nuestros objetivos.
- Reconocimiento público y remuneración económica ante el buen desempeño.
- Comunicación abierta para promover el trabajo en equipo.
- Innovación constante, iniciativa y creatividad para lograr productividad y eficiencia.
- Respeto a las personas, a la sociedad y al medio ambiente.

PANORAMA ACTUAL

Ecuacolor es una marca reconocida, posee una presencia bastante fuerte en el mercado fotográfico a nivel nacional, con más de 100 fototiendas. Ha llegado a poseer el 70% de participación del mercado.

- Es parte de un grupo económico conformado por Comandato, OndaPositiva, TecniPrint.
- Mucha de la infraestructura tecnológica es compartida por el Grupo Corporativo.
- Existen Niveles Gerenciales que cumplen sus funciones de manera Corporativo.

El mercado fotográfico en el Ecuador esta cambiando, el cambio se esta dando hacia el revelado digital, lo que motiva que el mercado de revelado tradicional se vea disminuido, afectando a los ingresos de la institución.

Para contrarrestar este efecto, la institución ha diseñado nuevas estrategias y desarrollado nuevas líneas de negocio.

Entre las estrategias de mas alto impacto están:

- Venta a Crédito, lo que debe incrementar la venta de Cámaras Digitales y otros productos de la línea Profesional.
- Se ha logrado obtener la representación exclusiva de los productos Maxell en todo el territorio nacional, de tal manera que se diversifican los ingresos que tiene la institución actualmente.
- Promociones para impulsar el revelado digital.
- Alianzas estratégicas con empresas nacionales para promociones cruzadas.
- Adquisición de Equipos de revelado digital PictureMaker.

Para lograr alcanzar los objetivos estratégicos definidos existen adquisiciones de tecnología que tienen una incidencia directa en el plan estratégicos de negocio.

- Adquisición de nuevo sistema de punto de ventas que cumpla los requerimientos de ley acorde a las necesidades y expectativas del negocio.
- Implementación de interconexión entre las principales tiendas a nivel nacional con la casa matriz.
- **<u>Administración de la tecnología actual que soporta los procesos del negocio. Siendo este ultimo uno de los pilares fundamentales en la consecución de las metas trazadas por la organización.</u>**

Los costos de estos proyectos son bastante significativos dentro de los resultados de la empresa, por eso razón la evaluación y adquisición de la tecnología antes mencionada debe ser llevada a cabo de la mejor manera posible.

PRODUCTOS CLAVES

- Cámaras digitales (KODAK, PANASONIC, NIKON)
- Rollos fotográficos (KODAK)
- Pilas
- Accesorios para cámaras y productos relacionados.

SERVICIOS CLAVES

- Revelado fotográfico.
- Ampliaciones.
- Montajes.
- Retoques
- Copias.

LINEAS DE NEGOCIO

Distribución.- Se encarga de la venta de mercadería y revelado al por mayor. Los distribuidores tienen líneas de crédito, descuentos, y promociones especiales.

Fototiendas.- Se encarga de la venta de mercadería al por menor y el revelado fotográficos.

CLIENTES

Fotógrafos.- Clientes que se dedican a la fotografía profesional, tienen descuentos y promociones especiales.

Distribuidores.- Clientes que están autorizados a vender mercadería, recibir trabajos de revelados y a facturarlos.

Aficionados.- Cliente que no se dedica a la fotografía como actividad profesional.

MERCADO.-

Ecuacolor esta enfocado en 2 segmentos, la venta a través de su cadena de retail y la venta a distribuidores.

Los principales competidores de Ecuacolor en el segmento de retail, son Konica, Fuji, Fybeca, otros quedan servicio de revelado. En lo que respecta a la distribución de Kodak y Maxell, es la misma que la de la marca a nivel internacional.

Actualmente la marca Ecuacolor esta catalogada como la numero uno en cuanto al revelado fotográfico y apunta a mantener esta posición. Ecuacolor siempre esta buscando la manera de incrementar su volumen de ventas, lanzando promociones. Sin embargo las ventas están disminuyendo debido a cambios que están surgiendo en el revelado tradicional, siendo esta la principal fuente de sus ingresos.

MARKETING Y PROMOCIONES.-

Constantemente se están lanzando promociones apuntando:

- Incrementar el revelado digital.
- Mantener el revelado tradicional.
- Incrementar la venta de productos KODAK y MAXELL.

Actualmente se han adquirido Impresoras Termales, Digitales, y equipos PICTURE Maker con el afán de soportar las diferentes promociones que son lanzadas consecutivamente.

ORGANIGRAMA DE LA EMPRESA.

Ver anexo A3.

Tecnología de Información.-

Existe un departamento de sistemas en Quito y Guayaquil, parte de los servicios de tecnología son provisto por el centro de computo de Comandato(Empresa del Grupo).

Entre los servicios tecnológicos que son provisto por el centro de computo de Comandato tenemos:

- Correo Interno.
- Acceso al Internet.
- Interconexión a través de micro-ondas con antenas de punto de vista en las fototiendas que están dentro de un almacén Comandato.
- Administración y soporte especializado de la red corporativa y base de datos.

Existe un Gerente de Sistemas que es corporativo, los Jefes del Dpto. de Informática de Quito y Guayaquil están subordinados a la Gerencia de Sistemas corporativas.

3.2 MARCO OPERATIVO.-

VENTAS, TÉRMINOS Y DESCUENTOS.

- La mercadería es recibida en las bodegas principales de Guayaquil, y de esta distribuida al resto del país.
- Las listas de precios, son creadas, administradas, aprobadas en la oficina principal.

Distribución

- Los precios de ventas para el área de distribución están formalmente definidos y aprobados por la alta gerencia.
- Existe el concepto de mercadería dada a consignación, pero con la aprobación de la gerencia general.
- Los descuentos son previamente pactados con el cliente y aprobados por la gerencia general cuando están fuera de los límites preestablecidos.
- Todas las ventas son a crédito.
- Todas las líneas de créditos son aprobadas, revisadas y analizadas para evitar la morosidad en la cartera.

Retail.

- Los precios de ventas para la cadena de retail, están clasificados por tipo de cliente (Aficionado y Fotógrafo), provincia, y en alguno casos por el nivel socio-económico del lugar en donde este ubicada la fototienda. Todos los precios son revisados y aprobados por la alta gerencia.
- Los descuentos están ya incluido en la lista de precios para el caso de los fotógrafos, y en el caso de los aficionados deben sujetarse al termino de la promoción a la que desean aplicar.
- Todas las ventas (actualmente) son en efectivo.

Semanalmente existen reuniones de los principales Gerentes de la Organización, para monitorear las tareas y actividades que se están llevando en cada área. Esto incluye información de: Antigüedad de Cartera, Política de Precios, Promociones, Programación de pedidos, Volúmenes de Venta, Estado de Resultados por tienda y línea de negocio. Cada gerencia es responsable de la información que se entrega.

Para garantizar el mejor trato al cliente, existe un Dpto. de atención al cliente en donde se lleva el detalle de cada reclamo y su respectiva solución. De la misma manera para garantizar que nuestra empresa de un buen trato a nuestros clientes, disponemos de medios de retroalimentación como: Cliente fantasma, Buzón de sugerencias, etc.

Nota: Ver Anexos A5 y A6 para detalle de los principales procesos.

COMPRAS DE INVENTARIO.-

- Nuestros mayores proveedores son Eastman Kodak, Maxell.
- La forma de costeo es por el método de promedio ponderado.
- El inventario es un rubro bastante significativo en el balance general de la institución.
- La Gerencia de Logística, Gerencia de Mercadeo, Jefe de Producción trabajan en conjunto para monitorear el inventario, y mantener un nivel adecuado a fin de satisfacer la demanda, por promociones y el proceso de revelado fotográfico.
- Adicionalmente la Gerencia de Logística se encarga de monitorear las importaciones, y de informar cualquier inconveniente directamente con la gerencia.

CUENTAS POR PAGAR.-

- La mayoría de las compras son de mercadería para la venta y materia prima para el proceso de revelado fotográfico.
- Existen contratos de arrendamientos por los locales que no son propios y están siendo usados por las fototiendas.
- Existen préstamos bancarios, pero no son de gran impacto en el estado financiero.
- Existen préstamos entre compañías del grupo.

Todas los cuentas por pagar son aprobados y monitoreadas. Para la aprobación existe una política bien definido por montos de compra. La información de las cuentas por porgar es semanalmente revisada e informada a la gerencia.

SALDOS DE EFECTIVO

- Todos los saldos en efectivo están en la moneda local.
- Transferencias importantes existen entre la administración de efectivos y las cuentas operacionales.
- El flujo de efectivo es diariamente monitorizado por la Gerencia Financiera.
- Las transferencias son aprobadas por la gerencia general.

PROPIEDADES, PLANTA & EQUIPOS.-

- Todas las propiedades, planta y equipos son de propiedad de la compañía(no es leasing financiero).
- La vida útil de todos los activos se basan en estándares de la industria y se deprecian por medio del método de línea recta.
- Si existen gastos significativos por reparación y mantenimiento.
- Durante los últimos 2 años, se han hecho importante adquisiciones en cuanto a equipos de revelado digital y termal.

3.3 INFORMACIÓN DEL AMBIENTE DE SISTEMA.

Los sistemas computacionales soportan todos los procesos del negocio, pero existen fototiendas que llevan sus transacciones de una forma manual debido a que el flujo de transacciones de la tienda y el flujo de efectivo de la empresa no justifica su automatización.

La información crítica de los estados financieros es generada por los sistemas computacionales.

El soporte y administración de la infraestructura de redes, sistema operativo, bases de datos es soportada por un tercero o por el centro de computo de COMANDATO. (Empresa del grupo).

Ecuacolor Laboratorio Fotográfico S.A. tiene las siguientes unidades de negocio:

- Venta en FotoTiendas.
- Venta a distribuidores.

Los principales procesos del negocio son:

- Ventas.
- Mercadeo.
- Producción. (Revelado Fotográfico)
- Logística
- Administración y control de fototiendas.
- Administración de fondos y flujo de efectivo.

3.3.1 CATALOGO DE APLICACIONES.

Aplicación	S.Operativo	Base de Datos	Procesos del Negocio que Soporta	Transaccionalidad
Sistema de Rol de Pagos.	Linux	PosgreSQL	Administración y Rendición de Cuentas.	MEDIA ALTA
Sistema Administrativo Financiero. (Contabilidad, Cxc, Cxp)	SCO Unix	Informix	Administración y Rendición de Cuentas.	MEDIA ALTA
Sistema de Administración de Inventario	SCO Unix	Informix	Facturación Distribuidores Facturación Retail. Administración de Inventario	ALTA
Sistema de Facturación a Distribuidores	SCO Unix	Informix	Facturación Distribuidores Administración de Inventario	MEDIA BAJA
Sistema de Compras Locales	SCO Unix	Informix	Adquisiciones Administración de Inventario	MEDIA
Sistema de Importaciones	SCO Unix	Informix	Adquisiciones Administración de Inventario	MEDIA
Sistema de Control de Caja	SCO Unix	Informix	Facturación Retail.	MEDIA ALTA
Sistema de Punto de Venta	W9x	FoxPro 2.6	Facturación Retail.	ALTA
Sistema de Información Gerencial.	SCO Unix	Informix	Toma de decisiones Gerenciales	BAJA
Sistema de Ordenes de Pago.	W2K	SQLServer	Administración y Rendición de Cuentas.	MEDIA

CATEGORIZACIÓN DE LA TRANSACCIONALIDAD DE LAS OPERACIONES.	
ALTA	Aproximadamente 200,000 Transacciones Mensuales
MEDIA ALTA	Aproximadamente 100,000 Transacciones Mensuales
MEDIA	Aproximadamente 50,000 Transacciones Mensuales

MEDIA BAJA	Aproximadamente 20,000 Transacciones Mensuales
BAJA	Aproximadamente 2,000 Transacciones Mensuales

3.3.2 RECURSO HUMANO – CENTRO DE COMPUTO

CARGO	CANTIDAD
Gerente Nacional de Sistemas	1
Jefes Departamentales (Guayaquil y Quito)	2
Analista Programadores (Guayaquil y Quito)	3
Help Desk(Guayaquil y Quito)	2

ORGANIGRAMA DE Tecnología de Información.

Ver anexo A4.

3.3.3 RECURSO TECNOLÓGICO

SOFTWARE.

- SCO Unix Open Server 5.0
- Linux RedHat Entreprise Server 3.x
- Lotus Domino 5.x.
- Office 2000 profesional.
- Visual Basic 6.0 Entreprise.
- JAVA 2 Standard Edition 1.4.
- SQL Server 2000.
- Informix Dynamic Server 9.x

HARDWARE.

- Servidor Principal (S.O. Sco Unix, 2 procesadores XEON, 1 GB de memoria, RAID 5, 4 fuentes redundantes, dispositivo de cinta magnética).
- Proxy Server (S.O. Linux, procesador PENTIUM 4, 512 MB)
- MAIL Server (S.O. Linux + Lotus Domino, procesador PENTIUM 4, 512 MB).
- Servidor de Desarrollo (S.O. Sco Unix, 1 procesadores XEON, 512 de memoria, dispositivo de cinta magnética).
- 240 PC en toda la organización.

RED.

- Cableado estructurado categoría 5 - 6.
- Red Inalámbrica.
- BACKBONE de comunicaciones.
- Conexión dial-up con fototiendas.

3.3.4 COMUNICACIÓN Y TRANSFERENCIA DE INFORMACIÓN A NIVEL DE LA ORGANIZACIÓN.-

- Existen 2 centros de cómputos: Quito y Guayaquil (Oficina Principal)

- La interconexión a través de Quito y Guayaquil es a través de un enlace dedicado de 256 kbps, usado por toda la organización.

- Los sistemas administrativos financieros y de producción tienen bases de datos separadas y ubicadas físicamente tanto en Quito como en Guayaquil, a través de un proceso nocturno se sincronizan las bases de datos.

- La interconexión y sincronización de datos entre las fototiendas y las oficinas principales ocurre una vez al día a través de un enlace telefónico.

3.3.5 ESTRATEGIA.

Tecnología de Información tiene entre sus principales proyectos:

- El soporte para la selección de un nuevo sistema de punto de venta a nivel nacional que permita a la empresa soportar las nuevas estrategias de negocio de la organización.
- La interconexión del 20% de sus fototiendas a nivela nacional para poder soportar la nueva línea de negocios y formas de negociación.

Cambios en Sistemas.

Ecuacolor esta considerando cambiar su sistema de punto de venta por exigencias del S.R.I, y por requerimientos de las nuevas estrategias del negocio. También existe un plan para la actualización de la base de datos y sistema operativos de los sistemas de la casa matriz.

4. MODELO DE MEJORES PRÁCTICAS UTILIZADO: COBIT

La Misión de CobiT:

Investigar , desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados , de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes y auditores.

Los Objetivos de Control para la Información y las Tecnologías Relacionadas (COBIT), ayuda a satisfacer las múltiples necesidades de la Administración estableciendo un puente entre los riesgos del negocio, los controles necesarios y los aspectos técnicos. Provee buenas prácticas a través de un dominio y el marco referencial de los procesos y presenta actividades en una estructura manejable y lógica. Las "Buenas prácticas" de COBIT reúne el consenso de expertos - quienes ayudarán a optimizar la inversión de la información y proporcionarán un mecanismo de medición que permitirá juzgar cuando las actividades van por el camino equivocado.

La Administración debe asegurar que los sistemas de control interno o el marco referencial están funcionando y soportan los procesos del negocio y debe tener claridad sobre la forma como cada actividad individual de control satisface los requerimientos de información e impacta los recursos de TI.

El impacto sobre los recursos de TI son resaltados en el M*arco de Referencia* de COBIT junto con los requerimientos del negocio que deben ser alcanzados:

- eficiencia
- efectividad
- confidencialidad
- integridad
- disponibilidad
- cumplimiento y
- confiabilidad de la información.

El control, que incluye políticas, estructuras, prácticas y procedimientos organizacionales, es responsabilidad de la administración. La administración, mediante este gobierno corporativo, debe asegurar que todos los individuos involucrados en la administración, uso, diseño, desarrollo, mantenimiento u operación de sistemas de información actúen con la debida diligencia.

Un Objetivo de Control en TI es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de TI.

La orientación al negocio es el tema principal de COBIT. Está diseñado no solo para ser utilizado por usuarios y auditores, sino que, lo más importante, esta diseñado para ser utilizado por los propietarios de los procesos de negocio como una guía clara y entendible. A medida que ascendemos, las prácticas de negocio requieren de una mayor delegación y empoderamiento de los dueños de los procesos para que estos tengan total responsabilidad de todos los aspectos relacionados con dichos procesos de negocio. En particular, esto incluye el proporcionar controles adecuados.

El *Marco de Referencia* de COBIT proporciona, al propietario de procesos de negocio, herramientas que facilitan el cumplimiento de esta responsabilidad. El *Marco de Referencia* comienza con una premisa simple y práctica:

" Con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos de TI agrupados en forma natural. "

El *Marco de Referencia* continúa con un conjunto de **34 *Objetivos de Control*** de alto nivel, uno para cada uno de los Procesos de TI, agrupados en cuatro dominios:

1. **Planeación y Organización,**
2. **Adquisición e Implementación**
3. **Entrega de servicios y Soporte y**
4. **Monitoreo.**

Esta estructura cubre todos los aspectos de información y de tecnología que la soporta. Administrando adecuadamente estos 34 Objetivos de Control de alto nivel, el propietario de procesos de negocio podrá asegurar que se proporciona un sistema de control adecuado para el ambiente de tecnología de información.

El *Marco de Referencia* de COBIT provee además una guía o lista de verificación para el Gobierno de TI. El Gobierno de TI proporciona las estructuras que encadenan los procesos de TI, los recursos de TI y la información con los objetivos y las estrategias de la empresa. El Gobierno de TI integra de una forma óptima el desempeño de la Planeación y Organización, la Adquisición e Implementación, la Entrega de Servicios y Soporte y el Monitoreo.

El Gobierno de TI facilita que la empresa obtenga total ventaja de su información y así mismo maximiza sus beneficios, capitalizando sus oportunidades y obteniendo ventaja competitiva

Adicionalmente, correspondiendo a cada uno de los 34 objetivos de control de alto nivel, existe una *Guía o directriz de Auditoría* o de aseguramiento que permite la revisión de los procesos de TI ***contra los 318 objetivos detallados*** de control recomendados por CobiT para proporcionar a la Gerencia la certeza de su cumplimiento y/o sugerencias para su mejoramiento.

Las Guías o Directrices Gerenciales de COBIT , desarrolladas recientemente, ayudan a la Gerencia a cumplir de una forma mas efectiva con las necesidades y requerimientos del Gobierno de TI. Las Directrices son acciones genéricas orientadas a proveer a la Administración la dirección para mantener bajo control la información de la empresa y sus procesos relacionados, para monitorear el logro de las metas organizacionales, para monitorear el desempeño de cada proceso de TI y para llevar a cabo un benchmarking de los logros organizacionales.

Específicamente COBIT provee **Modelos de Madurez** para el control sobre los procesos de TI de tal forma que la Administración puede ubicarse en el puntodonde la organización está hoy, donde está en relación con los "mejores de su clase" en su industria y con los estándares internacionales y así mismo determinar adonde quiere llegar;

Factores Críticos de Éxito (Critical Success Factors), que definen o determina cuales son las mas importantes directrices que deben ser consideradas por la Administración para lograr control sobre y dentro de los procesos de TI.

Indicadores Claves del logro / Objetivos o de Resultados (Key Goal Indicators) los cuales definen los mecanismos de medición que indicarán a la Gerencia—después del hecho– si un proceso de TI ha satisfecho los requerimientos del negocio; y los

Indicadores Clave de desempeño (Key Performance Indicators) los cuales son indicadoresprimarios que definen la medida para conocer qué tan bien se está ejecutando el proceso de TI frente o comparado contra el objetivo que se busca.

Las Directrices Gerenciales de COBIT son genéricas y son acciones orientadas al propósito de responder los siguientes tipos de preguntas gerenciales: ¿Qué tan lejos debemos ir y se justifica el costo respecto al beneficio obtenido? ¿Cuáles son los indicadores de buen desempeño? ¿Cuáles son los factores críticos de éxito? ¿Cuáles son los riesgos de no lograr nuestros objetivos? ¿Qué hacen otros? ¿Cómo nos podemos medir y comparar

COBIT contiene adicionalmente un ***Conjunto de Herramientas de Implementación*** que proporciona lecciones aprendidas por empresas que rápida y exitosamente aplicaron COBIT en sus ambientes de trabajo. Incluye dos herramientas particularmente útiles - Diagnóstico de Sensibilización Gerencial (Management Awareness Diagnostic) y Diagnóstico de Control en TI (IT Control Diagnostic) - para proporcionar asistencia en el análisis del ambiente de control de TI en una organización.

En los próximos años las Directivas de las Organizaciones necesitarán demostrar que están logrando incrementar sus niveles de seguridad y control. COBIT es una herramienta que ayuda a los Directivos a colocar un puente entre los requerimientos de control, los aspectos técnicos y los riesgos del negocio y adicionalmente informa a los accionistas o dueños de la empresa el nivel de control alcanzado. COBIT habilita el desarrollo de una política clara y de buenas prácticas de control de TI a través de las organizaciones, a nivel mundial.

Por lo tanto, COBIT está diseñado para ser la herramienta de gobierno de TI que ayude al entendimiento y a la administración de los riesgos así como de los beneficios asociados con la información y sus tecnologías relacionadas.

5. PROPUESTA METODOLÓGICA PARA EL DISEÑO DEL SGSI DE ECUACOLOR.

Existen dos clases distintas de modelos de control actualmente disponibles, aquéllos de la clase del "modelo de control de negocios" (por ejemplo COSO) y los "modelos más enfocados a TI" (por ejemplo, DTI). *COBIT* intenta cubrir la brecha que existe entre los dos. Debido a esto, COBIT se posiciona como una herramienta más completa para la Administración y para operar a un nivel superior a los estándares de tecnología para la administración de sistemas de información..

Por lo tanto, COBIT es el modelo para el gobierno de TI!

El marco metodológico conceptual para elaborar el diseño del Sistema de Gestión de la Seguridad de Ecuacolor Laboratorio Fotográfico S.A., usando el modelo de mejores prácticas COBIT, fue el siguiente:

1. Definición de los criterios de la Información
2. Seleccionar los criterios de la Información que están relacionados con Seguridad.
3. Seleccionar de los 34 procesos de COBIT, cuales son los procesos que son impactados de manera primaria por los criterios de la información relacionados con la seguridad.
4. Definir los Objetivos de Control detallados.
5. Aplicación del modelo de madurez, para determinar un estado de la situación actual de la empresa y cuales son sus metas, en cuanto a seguridad.
6. Realizar una evaluación y priorizacion de riesgos.
7. Elaborar los planes de acción que incluyen los controles, para poder mitigar los riesgos de alta y media exposición.

DEFINICIONES GENERALES

Para propósitos de este proyecto, se proporcionan las siguientes definiciones. La definición de "Control" está adaptada del reporte *COSO [Committee of Sponsoring Organisations of the Treadway Commission. Internal Control-Integrated Framework*, 1992 y la definición para "Objetivo de Control de TI" ha sido adaptada del reporte SAC (*Systems Auditability and Control Report, The Institute of Internal Auditors Research Foundation*, 1991 y 1994).

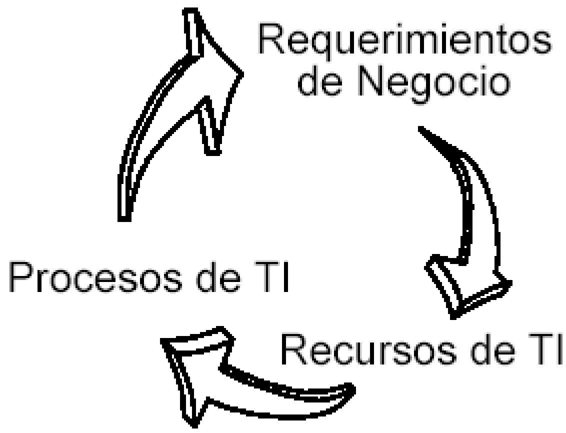
Control se define como.- Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos.

Objetivo de control en TI se define como.- Una sentencia del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de TI particular.

Gobierno de TI se define como.- Una estructura de relaciones y procesos para dirigir y controlar la empresa con el fin de lograr sus objetivos al añadir valor mientras se equilibran los riesgos contra el retorno sobre TI y sus procesos.

DEFINICIÓN DE LOS CRITERIOS DE LA INFORMACIÓN.

El concepto fundamental del *Marco Referencial de* COBIT se refiere a que el enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información que deben ser administrados por procesos de TI.



Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como *requerimientos de negocio para la información*. Al establecer la lista de requerimientos, *COBIT* combina los principios contenidos en los modelos referenciales existentes y conocidos:

Requerimientos de Calidad	Calidad Costo Entrega o Distribución (de servicio)
Requerimientos Fiduciarios (COSO)	Efectividad y eficiencia de las operaciones Confiabilidad de la información Cumplimiento de leyes y regulaciones
Requerimientos de Seguridad	Confidencialidad Integridad Disponibilidad

La Calidad ha sido considerada principalmente por su aspecto 'negativo' (ausencia de fallas, confiabilidad, etc.), lo cual también se encuentra contenido en gran medida en los criterios de Integridad. Los aspectos positivos, pero menos tangibles, de la calidad (estilo, atractivo, "ver y sentir", desempeño más allá de las expectativas, etc.) no fueron, por un tiempo, considerados desde un punto de vista de Objetivos de Control de TI. La premisa se refiere a que la primera prioridad deberá estar dirigida al manejo apropiado de los riesgos al compararlos contra las oportunidades. El aspecto utilizable de la Calidad está cubierto por los criterios de efectividad. Se consideró que el aspecto de entrega o distribución del servicio, de la Calidad se traslapa con el aspecto de disponibilidad correspondiente a los requerimientos de seguridad y también en alguna medida, con la efectividad y la eficiencia. Finalmente, el Costo también es considerado, siendo cubierto por la Eficiencia.

Para los requerimientos fiduciarios, COBIT no intentó reinventar la rueda – se utilizaron las definiciones de COSO para la efectividad y eficiencia de las operaciones, confiabilidad de información y cumplimiento con leyes y regulaciones. Sin embargo, confiabilidad de información fue ampliada para incluir toda la información – no sólo información financiera. **C**on respecto a los aspectos de **seguridad**, COBIT identificó la confidencialidad, integridad y disponibilidad como los elementos clave— se encontró que estos mismos tres elementos son utilizados a nivel mundial para describir los requerimientos de seguridad.
Comenzando el análisis a partir de los requerimientos de Calidad, Fiduciarios y de Seguridad más amplios, se extrajeron siete categorías distintas, ciertamente superpuestas. A continuación se muestran las definiciones utilizadas por COBIT:

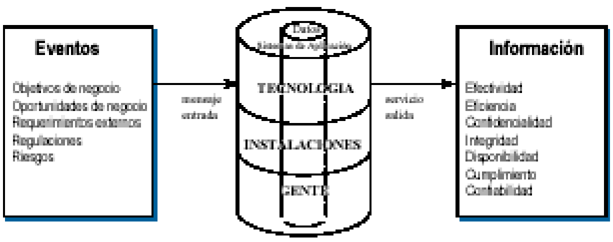
Efectividad	Información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
Eficiencia	Provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
Confidencialidad	Protección de información sensible contra divulgación no autorizada.
Integridad	Precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
Disponibilidad	Disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
Cumplimiento	Cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo criterios de negocio impuestos externamente.
Confiabilidad de la información	Provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Los recursos de TI identificados en COBIT pueden explicarse/ definirse como se muestra a continuación:

Datos	Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.
Aplicaciones	Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.
Tecnología	La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.
Instalaciones	Recursos para alojar y dar soporte a los sistemas de información.
Personas	Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

El dinero o capital no fue considerado como un recurso de TI para la clasificación de los objetivos de control porque el dinero puede ser considerado como una inversión dentro de cualquiera de los recursos presentados. Además debe anotarse que el *Marco Referencial* no se refiere específicamente a la documentación de todos los materiales relacionados con un proceso de TI en particular. Como un aspecto de buenas prácticas, la documentación es considerada como un buen control, y por lo tanto la falta de documentación sería causa de una mayor revisión y análisis de los controles compensatorios en cualquier área bajo revisión.

Otra forma de ver la relación de los recursos de TI con respecto a la entrega de servicios se describe a continuación:



CRITERIOS DE LA SEGURIDAD.-

Los criterios de la seguridad usados a nivel mundial por los modelos de mejores prácticas y estándares son los siguientes:

Confidencialidad	Protección de información sensible contra divulgación no autorizada.
Integridad	Precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
Disponibilidad	Disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

SELECCIÓN DE LOS PROCESOS DE COBIT RELACIONADOS CON EL DISEÑO DEL SGSI.-

Los Recursos de TI necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos.

Resulta claro que las medidas de control no satisfarán necesariamente los diferentes requerimientos de información del negocio en la misma medida.

Por esa razón los procesos en COBIT satisfacen uno o varios criterios de la información de la siguiente manera:

(P) Primario.- es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.

(S) 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; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

PROCESOS COBIT			
P01	Definir un plan estratégico de sistemas	DS1	Definir niveles de servicio
P02	Definir la arquitectura de información	DS2	Administrar servicios de terceros
P03	Determinar la dirección tecnológica	DS3	Administrar desempeño y capacidad
P04	Definir la organización y sus relaciones	DS4	Asegurar continuidad de servicio
P05	Administrar las inversiones (en TI)	DS5	Garantizar la seguridad de sistemas
P06	Comunicar la dirección y objetivos de la gerencia	DS6	Identificar y asignar costos
P07	Administrar los recursos humanos	DS7	Educar y capacitar a usuarios
P08	Asegurar el apego a disposiciones externas	DS8	Apoyar y orientar a clientes
P09	Evaluar Riesgos	DS9	Administrar la configuración
P010	Administrar Proyectos	DS10	Administrar problemas e incidentes
P011	Administrar Calidad	DS11	Administrar la información
		DS12	Administrar las instalaciones
AI1	Identificar soluciones de automatización	DS13	Administrar la operación
AI2	Adquirir y mantener software de aplicación		
AI3	Adquirir y mantener la arquitectura tecnológica	M1	Monitorear el proceso
AI4	Desarrollar y mantener procedimientos	M2	Evaluar lo adecuado del control interno
AI5	Instalar y acreditar sistemas de información	M3	Obtener aseguramiento independiente
AI6	Administrar cambios	M4	Proporcionar auditoria independiente

Matriz de Selección

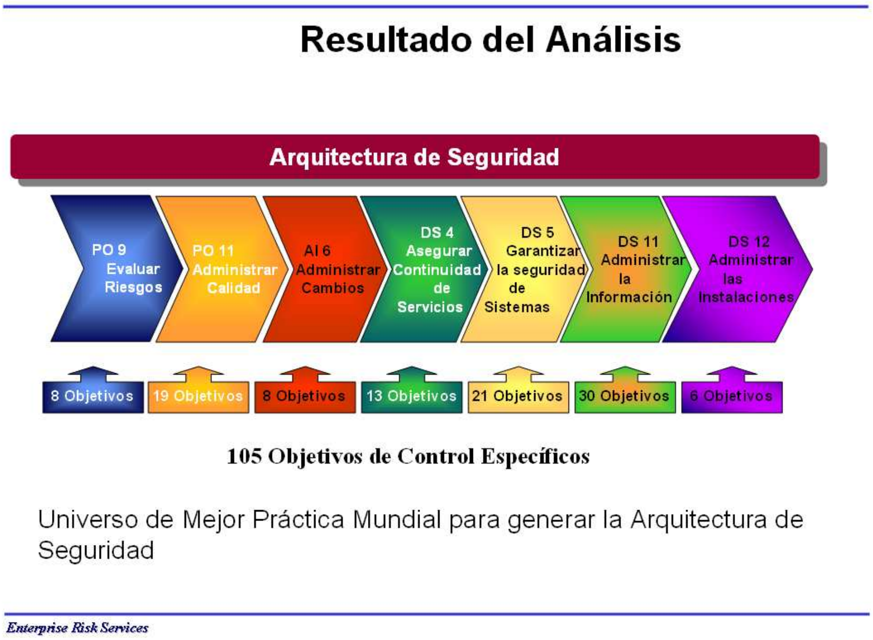
DOMINIO		PROCESO	efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad	recursos	sistemas de aplicación	tecnología	instalaciones	datos
			Criterios de Información							Recursos de TI				
Planeación y Organización	PO1	Definir un plan estratégico de sistemas	P	S						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

Matriz de Selección

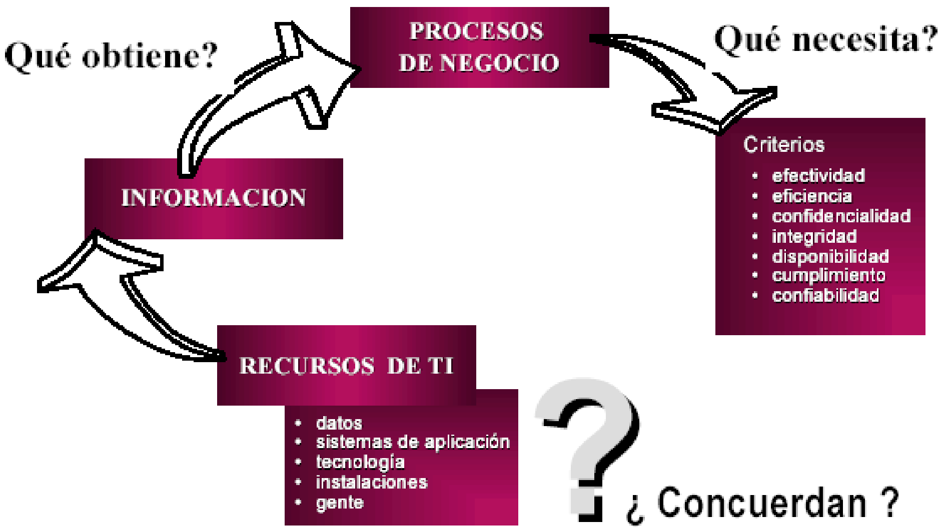
			Criterios de Información							Recursos de TI				
DOMINIO		PROCESO	efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad	recursos	sistemas de aplicación	tecnología	instalaciones	datos
Planeación y Organización	PO1	Definir un plan estratégico de sistemas	P	S						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

DEFINICIÓN DE LOS OBJETIVOS DE CONTROL.

Después de haber seleccionado los procesos que son afectados por los criterios de información de **Seguridad** (Confidencialidad, Integridad y Disponibilidad) de una manera primario, se obtienen los siguientes Objetivos de Control detallados:



Con el fin de asegurar que los requerimientos del negocio para la información se cumplan, es necesario definir, implementar y monitorear adecuadas medidas de control sobre esos recursos. ¿Cómo pueden entonces las empresas estar satisfechas respecto a que la información obtenida presente las características que necesitan? Es aquí donde se requiere de un sano marco referencial de Objetivos de Control para TI. El siguiente diagrama ilustra este concepto.



ARQUITECTURA DE SEGURIDAD.-

Objetivos de Control Detallados o Específicos.-

PROCESO	OBJETIVO DE CONTROL DETALLADO	CRITERIOS DE INFORMACIÓN	
		PRIMARIO	SECUNDARIO
PO9.- Evaluar Riesgo	• Evaluación de Riesgos del Negocio • Enfoque de Evaluación de Riesgos • Identificación de Riesgos • Medición de Riesgos • Plan de Acción contra Riesgos • Aceptación de Riesgos • Selección de Garantías o Protecciones • Compromiso con el Análisis de Riesgos	Efectividad Confidencialidad Integridad Disponibilidad	Eficiencia Cumplimiento Confiabilidad
PO11.- Administración de la calidad	• Plan General de Calidad. • Enfoque de Aseguramiento de Calidad. • Planeación del Aseguramiento de Calidad. • Revisión del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares y Procedimientos de TI. • Metodología del Ciclo de Vida de Desarrollo de Sistemas • Metodología del Ciclo de Vida de Desarrollo de Sistemas para Cambios Mayores a la Tecnología Actual • Actualización de la Metodología del Ciclo de Vida de Desarrollo de Sistemas. • Coordinación y Comunicación. • Marco de Referencia de Adquisición y Mantenimiento para la Infraestructura de Tecnología. • Relaciones con Terceras Partes como Implementadotes. • Estándares para la Documentación de Programas. • Estándares para Pruebas de Programas. • Estándares para Pruebas de Sistemas. • Pruebas Piloto/En Paralelo. • Documentación de las Pruebas del Sistema. • Evaluación del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares de Desarrollo. • Revisión del Aseguramiento de Calidad sobre el Logro de los Objetivos de TI. • Métricas de calidad. • Reportes de Revisiones de Aseguramiento de Calidad.	Efectividad Eficiencia Integridad	Confiabilidad

PROCESO	OBJETIVO DE CONTROL DETALLADO	CRITERIOS DE INFORMACIÓN	
		PRIMARIO	SECUNDARIO
AI6.- Administrar cambios.	• Inicio y Control de Solicitudes de Cambio • Análisis de Impacto • Control de Cambios • Cambios de Emergencia • Documentación y Procedimientos • Mantenimiento Autorizado • Política de Liberación de Software • Distribución de Software	Efectividad Eficiencia Integridad	Confiabilidad
DS4.- Asegurar el servicio continuo	• Marco de Referencia de Continuidad de Tecnología de información • Estrategia y Filosofía del Plan de Continuidad de TI • Contenido del Plan de Continuidad de TI. • Reducción de requerimientos de Continuidad de Tecnología de Información. • Mantenimiento del Plan de Continuidad de Tecnología de Información. • Pruebas del Plan de Continuidad de TI. • Entrenamiento sobre el Plan de Continuidad de Tecnología de Información. • Distribución del Plan de Continuidad de TI. • Procedimientos de respaldo de procesamiento alternativo para Departamentos usuarios. • Recursos Críticos de Tecnología de Información. • Sitio y Hardware de Respaldo. • Almacenamiento de respaldo en el sitio alterno (Off-site). • Procedimiento de afinamiento del Plan de Continuidad.	Efectividad Disponibilidad	Eficiencia
DS5.- Garantizar la seguridad de los sistemas.	• Administrar Medidas de Seguridad. • Identificación, Autenticación y Acceso. • Seguridad de Acceso a Datos en Línea. • Administración de Cuentas de Usuario. • Revisión Gerencial de Cuentas de Usuario. • Control de Usuarios sobre Cuentas de Usuario. • Vigilancia de Seguridad. • Clasificación de Datos. • Administración de Derechos de Acceso e Identificación Centralizada. • Reportes de Violación y de Actividades de Seguridad. • Manejo de Incidentes.	Confidencialidad Integridad	Disponibilidad Cumplimiento Confiabilidad

<table>
<tr><th rowspan="2">PROCESO</th><th rowspan="2">OBJETIVO DE CONTROL DETALLADO</th><th colspan="2">CRITERIOS DE INFORMACIÓN</th></tr>
<tr><th>PRIMARIO</th><th>SECUNDARIO</th></tr>
<tr><td>DS5.- Garantizar la seguridad de los sistemas.</td><td>• Reacreditación.
• Confianza en Contrapartes.
• Autorización de transacciones.
• No negación o no rechazo.
• Sendero Seguro.
• Protección de las funciones de seguridad.
• Administración de Llaves Criptográficas.
• Prevención, Detección y Corrección de Software “Malicioso”.
• Arquitectura de Firewalls y conexión a redes públicas.
• Protección de Valores Electrónicos.</td><td>Confidencialidad
Integridad</td><td>Disponibilidad
Cumplimiento
Confiabilidad</td></tr>
<tr><td>DS11.- Administración de datos</td><td>• Procedimientos de Preparación de Datos.
• Procedimientos de Autorización de Documentos Fuente.
• Recopilación de Datos de Documentos Fuente.
• Manejo de errores de documentos fuente.
• Retención de Documentos Fuente.
• Procedimientos de Autorización de Entrada de Datos.
• Chequeos de Exactitud, Suficiencia y Autorización.
• Manejo de Errores en la Entrada de Datos.
• Integridad de Procesamiento de Datos.
• Validación y Edición de Procesamiento de Datos.
• Manejo de Errores en el Procesamiento de Datos.
• Manejo y Retención de Datos de Salida.
• Distribución de Datos Salidos de los Procesos.
• Balanceo y Conciliación de Datos de Salida.
• Revisión de Datos de Salida y Manejo de Errores.
• Provisiones de Seguridad para Reportes de Salida.
• Protección de Información Sensible durante transmisión y transporte.
• Protección de Información Sensitiva Desechada.
• Administración de Almacenamiento.
• Períodos de Retención y Términos de Almacenamiento.</td><td>Integridad
Confiabilidad</td><td></td></tr>
</table>

PROCESO	OBJETIVO DE CONTROL DETALLADO	CRITERIOS DE INFORMACIÓN	
		PRIMARIO	SECUNDARIO
DS11.- Administración de datos	• Sistema de Administración de la Librería de Medios • Responsabilidades de la Administración de la Librería de Medios • Respaldo (Back-up) y Restauración • Funciones de Respaldo • Almacenamiento de Respaldos • Archivo • Protección de Mensajes Sensitivos • Autenticación e Integridad • Integridad de Transacciones Electrónicas • Integridad Continua de Datos Almacenados	Integridad Confiabilidad	
DS12.-Administración de instalaciones.	• Seguridad Física • Discreción sobre las Instalaciones de Tecnología de Información • Escolta de Visitantes • Salud y Seguridad del Personal • Protección contra Factores Ambientales • Suministro Ininterrumpido de Energía	Integridad Disponibilidad	

MODELO DE MADUREZ.-

El enfoque de los Modelos de Madurez para el control sobre los procesos de TI consiste en desarrollar un método de asignación de puntos para que una organización pueda calificarse desde Inexistente hasta optimizada (de 0 a 5). Este planteamiento se basa en el Modelo de Madurez que el Software Engineering Institute definió para la madurez de la capacidad de desarrollo de software. Cualquiera sea el modelo, las escalas no deben estar demasiado simplificadas, lo que haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable.

En contraste, uno debe concentrarse en los niveles de madurez basándose en un conjunto de condiciones que pueden ser satisfechas de una forma que no sea ambigua. En comparación con los niveles desarrollados para cada uno de los 34 procesos de TI de COBIT, la administración puede mapear:

- La situación actual de la organización—dónde está la organización actualmente
- La estrategia de la organización para mejoramiento—dónde quiere estar la organización

El modelo de madurez aplicado a Ecuacolor Laboratorio Fotográfico S.A. lo puede encontrar mas adelante en este documento.

EVALUACIÓN Y PRIORIZACION DE RIESGOS.-

Para asegurar que la Gerencia alcance los objetivos de negocios, ésta debe dirigir y administrar las actividades de TI para alcanzar un balance efectivo entre el manejo de riesgos y los beneficios encontrados. Para cumplir esto, la Gerencia necesita identificar las actividades mas importantes que deben ser desarrolladas, midiendo el progreso hacia el cumplimiento de las metas y determinando que tan bien se están desarrollando los procesos de TI. Aun mas, necesita tener la habilidad de avaluar el nivel de madurez de la organización contra las mejores practicas industriales y los modelos internacionales.

La evaluación y priorizacion de riesgos aplicado a Ecuacolor Laboratorio Fotográfico S.A. lo puede encontrar mas adelante en este documento.

PLANES DE ACCIÓN.-

Los controles que se sugieren implementar para mitigar los riesgos identificados en la fase de "evaluación y priorizacion de riesgos", así como sus responsables y tiempos aproximados de implementación se pueden encontrar en los planes de acción.

Los planes de acción del Sistema de Seguridad de la Información aplicados a Ecuacolor Laboratorio Fotográfico S.A. lo puede encontrar mas adelante en este documento.

6 MODELO DE MADUREZ DE LOS 7 PROCESOS DE SEGURIDAD DE INFORMACIÓN

A los gerentes generales de las organizaciones corporativas y públicas se les pide frecuentemente que consideren un caso de negocio para los gastos de recursos para controlar la infraestructura de información. Mientras pocos argumentarían que esto no es bueno, todos se deben preguntar:

"¿Hasta dónde debemos ir, y está el costo justificado por el beneficio?"

Para ayudar a responder esa pregunta, a menudo se hacen otras preguntas relacionadas:

"¿Qué estándares reconocidos internacionalmente existen, y cómo estamos nosotros situados respecto a éstos?

"¿Qué están haciendo los demás, y cómo estamos nosotros situados en relación a ellos?"

"¿Qué está considerado como la mejor práctica de la industria, y cómo estamos nosotros situados en relación con esa mejor práctica?"

"Basados en estas comparaciones externas, podría decirse que nosotros estamos tomando precauciones "razonables"para salvaguardar nuestros activos de información?"

Usualmente ha sido difícil dar respuestas sensatas a estas preguntas, porque no se ha contado con las herramientas requeridas para hacer las evaluaciones necesarias.

La administración de TI está constantemente en la búsqueda de herramientas de referencia y de auto evaluación en respuesta a la necesidad de saber qué hacer en una forma eficiente. Comenzando con los procesos de COBIT y con objetivos de control de alto nivel, el propietario del proceso debe ser capaz de llevar a cabo cada vez mayores Benchmark en comparación con dicho objetivo de control. Esto satisface tres necesidades:

(1) una medida relativa de dónde está la organización
(2) una forma de decidir eficientemente dónde ir
(3) una herramienta para medir el progreso con respecto al objetivo

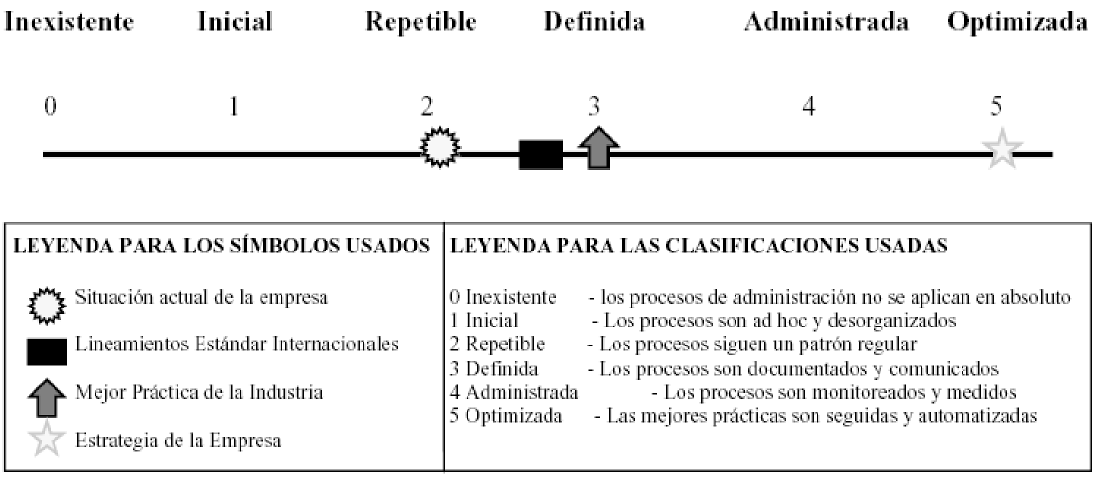
El *Marco Referencial* de COBIT define 34 procesos de TI dentro de un entorno de TI.
Para cada proceso hay una expresión de control de alto nivel y entre 3 y 30 objetivos detallados de control. El propietario del proceso debe ser capaz de determinar el nivel de cumplimiento de los objetivos de control ya sea como una rápida auto evaluación o como una referencia en conjunto con una revisión independiente. Cualquiera de estas evaluaciones que la administración pueda desear poner en contexto comparando con la industria y con el entorno en que ellas se encuentran o en comparación con dónde están evolucionando los estándares y las reglamentaciones internacionales (por ejemplo, las futuras expectativas que surgen). Para que los resultados se puedan utilizar fácilmente en los reportes de la administración, donde ellos serán presentados como un medio para

respaldar el caso de negocio para planes futuros, es necesario suministrar un método gráfico de presentación.

El enfoque de los Modelos de Madurez para el control sobre los procesos de TI consiste en desarrollar un método de asignación de puntos para que una organización pueda calificarse desde Inexistente hasta optimizada (de 0 a 5). Este planteamiento se basa en el Modelo de Madurez que el Software Engineering Institute definió para la madurez de la capacidad de desarrollo de software. Cualquiera sea el modelo, las escalas no deben estar demasiado simplificadas, lo que haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable.

En contraste, uno debe concentrarse en los niveles de madurez basándose en un conjunto de condiciones que pueden ser satisfechas de una forma que no sea ambigua. En comparación con los niveles desarrollados para cada uno de los 34 procesos de TI de COBIT, la administración puede mapear:

- La situación actual de la organización—dónde está la organización actualmente
- La situación actual de la industria (la mejor de su clase en)—la comparación
- La situación actual de los estándares internacionales—comparación adicional
- La estrategia de la organización para mejoramiento—dónde quiere estar la organización



Para cada uno e los 34 procesos de TI, hay una escala gradual ascendente de medidas, basada en una clasificación de “0” hasta “5”. La escala está asociada con las descripciones del modelo genérico cualitativo de madurez que van desde “Inexistente” hasta “Optimizada” de la forma siguiente:

MODELO GENÉRICO DE MADUREZ
0 Inexistente. Total falta de un proceso reconocible. La organización ni siquiera ha reconocido que hay un problema que resolver.
1 Inicial. Hay evidencia de que la organización ha reconocido que los problemas existen y que necesitan ser re sueltos. Sin embargo, no hay procesos estandarizados pero en cambio hay métodos ad hoc que tienden a ser aplicados en forma individual o caso por caso. El método general de la administración es desorganizado.
2 Repetible. Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.
3 Definida. Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.
4 Administrada. Es posible monitorear y medir el cumplimiento de los procedimientos y emprender acción donde los procesos parecen no estar funcionando efectivamente. Los procesos están bajo constante
mejoramiento y proveen buena práctica. Se usan la automatización y las herramientas en una forma limitada o fragmentada.
5 Optimizada. Los procesos han sido refinados hasta un nivel de la mejor práctica, basados en los resultados de mejoramiento continuo y diseño de la madurez con otras organizaciones. TI se usa en una forma integrada para automatizar el flujo de trabajo, suministrando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte con rapidez.

COBIT es un marco de referencia general dirigido a la administración de TI y como tal estas escalas necesitan ser prácticas para aplicar y razonablemente fáciles de entender. Sin embargo, los tópicos de riesgo y de control apropiado en los procesos de administración de TI son inherentemente subjetivos e imprecisos y no necesitan el enfoque menos automatizado que se encuentra en los modelos de madurez para la ingeniería de software.

La ventaja de un enfoque de Modelo de Madurez es que es relativamente fácil para la administración ponerse en la escala y apreciar lo que está involucrado si necesita mejorar el desempeño. La escala incluye 0 a 5 porque es bastante probable que no exista ningún proceso en absoluto. La escala 0-5 se basa en una escala simple de madurez que muestra cómo evoluciona un proceso desde Inexistente hasta optimizado. Debido a que son procesos de administración, la madurez y la capacidad aumentada es también sinónimo de mayor manejo del riesgo y mayor eficiencia.

El Modelo de Madurez es una forma de medir qué tan bien desarrollados están los procesos de administración. El grado de desarrollo que deben tener depende de las necesidades del negocio, como se menciona aquí anteriormente. Las escalas son sólo ejemplos prácticos para un proceso dado de administración que muestra esquemas típicos para cada nivel de madurez. Los Criterios de Información ayudan a asegurarse de que estamos enfocados en los aspectos correctos de la administración cuando describimos la práctica real. Por ejemplo, la planificación y organización están enfocadas en los objetivos de efectividad y eficiencia de administración, mientras que asegurar la seguridad de los sistemas se enfocará en el manejo de la confidencialidad y la integridad.

Las escalas del Modelo de Madurez ayudarán al profesional a explicar a los administradores dónde existen deficiencias en la administración de TI y a fijarse objetivos para donde necesitan estar comparando las prácticas de control de su organización con los ejemplos de la mejor práctica. El nivel correcto de madurez estará influenciado por los objetivos de negocio y el entorno operativo de la empresa. Específicamente, el nivel de madurez de control dependerá de la dependencia de TI que tenga la empresa, de la sofisticación de la tecnología y, lo que es más importante, del valor de su información.

Un punto estratégico de referencia para que una organización mejore la seguridad y el control podría consistir también en mirar las normas internacionales que surgen y las mejores prácticas de su clase. Las prácticas actuales que surgen pueden llegar a ser el nivel esperado de desempeño de mañana y es por lo tanto útil para planificar dónde quiere una organización estar en el tiempo.

Los Modelos de Madurez se construyen a partir del modelo genérico cualitativo (ver arriba) a los que se agregan las prácticas y los principios de los dominios siguientes de forma creciente a través de todos los niveles:

- Entendimiento y conocimiento de los riesgos y de los problemas de control
- Capacitación y comunicación aplicadas a los problemas
- Proceso y prácticas que son implementados
- Técnicas y automatización para hacer los procesos más efectivos y eficientes
- Grado de cumplimiento de la política interna, las leyes y las reglamentaciones
- Tipo y grado de pericia empleada.

La tabla siguiente describe esta creciente aplicación de prácticas a través de todos los niveles para los distintos tópicos. Junto con el modelo cualitativo, constituye un modelo genérico de madurez aplicable a la mayoría de los procesos de TI.

	Entendimiento y Conocimiento	Capacitación y Comunicación	Proceso y Prácticas	Técnicas y Automatización	Cumplimiento	Pericia
1	Reconocimiento	Comunicación esporádica sobre los problemas	Enfoque ad hoc del proceso y de la práctica			
2	Conocimiento/ concientización	Comunicación sobre el problema general y las necesidades	Surge un proceso similar/ común pero intuitivo	Están apareciendo Herramientas comunes.	Monitoreo inconsistente de Problemas aislados	
3	Entendimiento de la necesidad de actuar	La capacitación informal soporta las iniciativas individuales	Las prácticas son definidas, estandarizadas y documentadas; se comienzan a compartir las mejores prácticas.	El conjunto de herramientas es estandarizado; se usan y se hacen valer las prácticas Disponibles actualmente.	Monitoreo inconsistente; surge la medición; el Balanced Store-card se adopta ocasionalmente; el análisis de las causas originarias es intuitivo.	Participación De Especialistas de TI en los procesos del negocio.
4	Entender todos los requerimientos	La capacitación formal soporta un programa administrado	La propiedad y las Responsabilidades del proceso están fijadas; el proceso es correcto y completo; se aplican las mejores prácticas.	Se usan técnicas maduras; se imponen las Herramientas estándar; uso limitado táctico de la tecnología.	Los Balanced scorecards se usan en algunas áreas; se señalan las excepciones; el análisis de las causas originarias está estandarizado	Participación de todos los expertos de Dominio interno.
5	Entendimiento avanzado, con perspectiva futura	La capacitación Y las Comunicaciones soportan las mejores prácticas externas y usan conceptos de vanguardia	Se aplican las mejores prácticas externas.	Se despliegan Técnicas sofisticadas; uso Extensivo optimizado de la tecnología	El Balanced scorecards seaplica globalmente; las Excelciones se Señalan de manera consistente y se actúa sobre las mismas; el análisis de las causas originarias se aplica siempre	Uso de Expertos externos y de líderes de la industria Para orientación.

En resumen, Los Modelos de Madurez:

- Se refieren a los requerimientos del negocio y a los aspectos posibilitadores en los diferentes niveles de madurez
- Son una escala que se presta para la comparación pragmática
- Son una escala en la que la diferencia puede hacerse mensurable de manera sencilla
- Son reconocibles como un "perfil" de la empresa relativo al gobierno de TI, la seguridad y el control
- Ayudan a fijar posiciones de "Como está" y "Como debe estar" en relación con el gobierno de TI, la madurez de la seguridad y el control

  Se prestan para hacer análisis de los vacíos/gap para determinar lo que es necesario hacer para alcanzar un nivel determinado
- Evitan, donde es posible, niveles discretos que crean umbrales que son difíciles de cruzar
- Aplican cada vez más factores críticos de éxito
- No son específicos de la industria ni son siempre aplicables, el tipo de negocio define lo que es apropiado.

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 1/2</td></tr>
<tr><td colspan="4">MODELO DE MADUREZ</td></tr>
<tr><td colspan="2">DOMINIO: PLANEACION Y ORGANIZACIÓN</td><td colspan="2">PO9.- Evaluar los Riesgos</td></tr>
<tr><td colspan="4">OBJETIVO DE CONTROL</td></tr>
<tr><td colspan="4">Control sobre el proceso de TI Evaluar los Riesgos con el objetivo del negocio de apoyar las decisiones de la administración en alcanzar los objetivos de TI y en responder a las amenazas reduciendo la complejidad, aumentando la objetividad e identificando factores de decisión importantes.</td></tr>
<tr><td>Estado Actual :</td><td>2</td><td>Estado Proyectado:</td><td>4</td></tr>
<tr><td colspan="4">CRITERIOS DE CALIFICACIÓN</td></tr>
<tr><td>0</td><td colspan="3">Inexistente La estimación del riesgo para los procesos y las decisiones del negocio no ocurre. La organización no considera los impactos del negocio asociados con vulnerabilidades de la seguridad y con inseguridades de proyectos de desarrollo. Es improbable que la administración de riesgos sea identificada dentro del plan de un proyecto o sea asignada a administradores específicos involucrados en el proyecto. La administración de TI no especifica responsabilidad para la administración del riesgo en las descripciones de los puestos de trabajo u otro medio informal. Riesgos específicos relacionados con TI como la seguridad, disponibilidad e integridad son considerados ocasionalmente por proyecto.</td></tr>
<tr><td>1</td><td colspan="3">Inicial /Ad Hoc La organización está conciente de sus responsabilidades y obligaciones legales y contractuales, pero considera los riesgos de TI de manera ad hoc, sin seguir procesos o políticas definidas. Tienen lugar evaluaciones informales del riesgo de proyecto a medida que lo determina cada proyecto. No es probable que las evaluaciones de riesgo sean identificadas específicamente dentro del plan de un proyecto o a ser asignado a administradores específicos involucrados en el proyecto. La administración de TI no especifica responsabilidad por la administración del riesgo en las descripciones de puestos de trabajo u otro medio informal. Los riesgos específicos relacionados con TI como son la seguridad, disponibilidad e integridad son ocasionalmente considerados por proyecto. Los riesgos relacionados con TI que afectan las operaciones cotidianas se discuten con poca frecuencia en las reuniones de la administración. Cuando se han considerado los riesgos, la mitigación es inconsistente.</td></tr>
<tr><td>2</td><td colspan="3">Repetible pero Intuitivo Ha surgido un entendimiento de que los riesgos de TI son importantes y que es necesario considerarlos. Existe algún enfoque de evaluación de riesgos, pero el proceso es todavía inmaduro y está en desarrollo. La evaluación es usualmente a un nivel elevado y típicamente se aplica sólo a los proyectos importantes. La evaluación de las operaciones en curso depende principalmente de los administradores de TI que lo presentan como un punto de la agenda, lo cual a menudo sólo ocurre cuando surgen problemas. La administración de TI generalmente no tiene definidos procedimientos o descripciones de puestos de trabajo que se encarguen de la administración del riesgo.</td></tr>
</table>

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 2/2</td></tr>
<tr><td colspan="4">MODELO DE MADUREZ</td></tr>
<tr><td colspan="2">DOMINIO: PLANEACION Y ORGANIZACIÓN</td><td colspan="2">PO9.- Evaluar los Riesgos</td></tr>
<tr><td colspan="4">OBJETIVO DE CONTROL</td></tr>
<tr><td colspan="4">Control sobre el proceso de TI Evaluar los Riesgos con el objetivo del negocio de apoyar las decisiones de la administración en alcanzar los objetivos de TI y en responder a las amenazas reduciendo la complejidad, aumentando la objetividad e identificando factores de decisión importantes.</td></tr>
<tr><td>Estado Actual :</td><td>2</td><td>Estado Proyectado:</td><td>4</td></tr>
<tr><td colspan="4">CRITERIOS DE CALIFICACIÓN</td></tr>
<tr><td>3</td><td colspan="3">Proceso Definido La política de manejo del riesgo a nivel de toda una organización define cuándo y cómo llevar a cabo evaluaciones de riesgo. La evaluación del riesgo sigue un proceso definido que está documentado y disponible para todo el persona a través de entrenamiento. Las decisiones de seguir el proceso y recibir entrenamiento se dejan a la discreción de las personas. La metodología es convincente y saludable, y asegura que los riesgos clave del negocio probablemente sean identificados. Las decisiones de seguir el proceso se dejan a los administradores individuales de TI y no hay procedimiento para asegurar que todos los proyectos estén cubiertos o que la operación en curso es examinada en busca de riesgos de manera regular.</td></tr>
<tr><td>4</td><td colspan="3">Administrado y Medible La evaluación del riesgo es un procedimientos estándar y las excepciones a seguir el procedimiento serían anunciadas por la administración de TI. Es probable que la administración del riesgo sea una función definida de la administración con responsabilidad a nivel general. El proceso es adelantado y el riesgo es evaluado a nivel del proyecto individual y también regularmente respecto a la operación general de TI. Se advierte a la administración sobre los cambios en el entorno de TI que podrían afectar significativamente los escenarios de riesgo como por ejemplo una mayor amenaza proveniente de la red o tendencias técnicas que afectan la integridad de la estrategia de TI. La administración puede monitorear la posición de riesgo y tomar decisiones inteligentes respecto a la exposición que está dispuesta a aceptar. La gerencia general ha determinado los niveles de riesgo que la organización tolerará y tiene medidas estándar de proporciones de riesgo / rendimiento. Presupuestos de administración para proyectos de administración de riesgos operativos para reevaluar los riesgos regularmente. Está establecida una base de datos de administración de riesgos.</td></tr>
<tr><td>5</td><td colspan="3">Optimizado La evaluación de los riesgos se ha desarrollado hasta una etapa en que un proceso estructurado, en toda la organización, es ejecutado, seguido y bien administrado. La tormenta de ideas y el análisis de la causa que originó el riesgo, que involucra a personas expertas, se aplican en toda la organización. La captura, análisis y reporte de datos de administración de riesgos están altamente automatizados. El asesoramiento se obtiene de los jefes en el terreno y la organización de TI participa en grupos colegas para intercambiar experiencias. La administración del riesgo está verdaderamente integrada en todas las operaciones y negocios de TI, es bien aceptada e involucra extensamente a los usuarios de servicios de TI.</td></tr>
</table>

<table>
<tr><th colspan="5">MODELO DE MEJORES PRACTICAS - COBIT</th></tr>
<tr><td colspan="3">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="4">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 1/1</td></tr>
<tr><td colspan="5">MODELO DE MADUREZ</td></tr>
<tr><td colspan="3">DOMINIO: PLANEACION Y ORGANIZACIÓN</td><td colspan="2">PO11.- Administrar Calidad</td></tr>
<tr><td colspan="5">OBJETIVO DE CONTROL</td></tr>
<tr><td colspan="5">Control sobre el proceso de TI Administrar la Calidad con el objetivo del negocio de satisfacer los requerimientos de TI del cliente.</td></tr>
<tr><td colspan="2">Estado Actual :</td><td>2</td><td>Estado Proyectado:</td><td>3</td></tr>
<tr><td colspan="5">CRITERIOS DE CALIFICACIÓN</td></tr>
<tr><td>0</td><td colspan="4">Inexistente La organización no ha reconocido que existe un problema que debe ser reconocido.</td></tr>
<tr><td>1</td><td colspan="4">Inicial /Ad Hoc Hay evidencia de que la organización ha reconocido que los problemas existen y que necesitan ser resueltos. Sin embargo, no hay procesos estandarizados pero en cambio hay métodos ad hoc que tienden a ser aplicados en forma individual o caso por caso. El método general de la administración es desorganizado.</td></tr>
<tr><td>2</td><td colspan="4">Repetible pero Intuitivo Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.</td></tr>
<tr><td>3</td><td colspan="4">Proceso Definido Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la formalización de las prácticas existentes.</td></tr>
<tr><td>4</td><td colspan="4">Administrado y Medible Es posible monitorear y medir el cumplimiento de los procedimientos y emprender acción donde los procesos parecen no estar funcionando efectivamente. Los procesos están bajo constante mejoramiento y proveen buena práctica. Se usan la automatización y las herramientas en una forma limitada o fragmentada.</td></tr>
<tr><td>5</td><td colspan="4">Optimizado Los procesos han sido refinados hasta un nivel de la mejor práctica, basados en los resultados de mejoramiento continuo y diseño de la madurez con otras organizaciones. TI se usa en una forma integrada para automatizar el flujo de trabajo, suministrando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte con rapidez.</td></tr>
</table>

<table>
<tr><td colspan="5">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="3">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="4">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 1/2</td></tr>
<tr><td colspan="5">MODELO DE MADUREZ</td></tr>
<tr><td colspan="3">DOMINIO: ADQUISICIÓN E IMPLEMENTACIÓN</td><td colspan="2">AI6.- Administrar Cambios</td></tr>
<tr><td colspan="5">OBJETIVO DE CONTROL</td></tr>
<tr><td colspan="5">El control sobre el proceso de TI Administrar Cambios de TI con el objetivo del negocio de minimizar la probabilidad de interrupción, alteraciones no autorizadas y errores</td></tr>
<tr><td colspan="2">Estado Actual :</td><td>2</td><td>Estado Proyectado:</td><td>4</td></tr>
<tr><td colspan="5">CRITERIOS DE CALIFICACIÓN</td></tr>
<tr><td>0</td><td colspan="4">Inexistente. No hay un proceso definido de administración de cambios y se pueden hacer cambios prácticamente sin control alguno. No hay conciencia de que los cambios pueden causar interrupciones tanto para TI como para las operaciones de negocios, y ninguna conciencia de los beneficios de una buena administración de cambios.</td></tr>
<tr><td>1</td><td colspan="4">Inicial /Ad hoc Se reconoce que los cambios deben ser administrados y controlados, pero no hay un proceso consistente para seguimiento. Las prácticas varían y es probable que ocurran cambios no autorizados. Hay documentación insuficiente o inexistente de cambios, y la documentación de configuración está incompleta y no es confiable. Es probable que ocurran errores junto con interrupciones en el entorno de producción causados por una administración deficiente del cambio.</td></tr>
<tr><td>2</td><td colspan="4">Repetible pero Intuitiva Hay un proceso informal de administración de cambios y la mayoría de los cambios siguen este método; sin embargo, el mismo no está estructurado, es rudimentario y está propenso a error. La precisión de la documentación de configuración es inconsistente y sólo tiene lugar una planeación y un estudio de impacto limitados antes de un cambio. Hay considerable ineficiencia y repetición de trabajo.</td></tr>
<tr><td>3</td><td colspan="4">Proceso Definido Está establecido un proceso formal de administración de cambios, que incluye procedimientos de categorización, priorización, emergencia, autorización y administración de cambios, pero no se impone su cumplimiento. El proceso definido no siempre es visto como adecuado o práctico y, en consecuencia, ocurren trabajos paralelos y los procesos son desviados. Es probable que ocurran errores y los cambios no autorizados ocurrirán ocasionalmente. El análisis de impacto a los cambios de TI sobre las operaciones del negocio se están volviendo formales para soportar la ejecución de los planes para nuevas aplicaciones y tecnologías.</td></tr>
<tr><td>4</td><td colspan="4">Administrado y Medible El proceso de administración de cambios está bien desarrollado y es seguido de manera consistente para todos los cambios, y la administración confía en que no hay excepciones. El proceso es eficiente y efectivo, pero se basa en considerables procedimientos y controles manuales para asegurar que se logre la calidad. Todos los cambios están sujetos a una planeación y estudio de impacto exhaustivos para minimizar la probabilidad de problemas posteriores a la producción. Está establecido un proceso de aprobación para los cambios. La documentación de administración de cambios está al día y es correcta, y los cambios son rastreados formalmente. La documentación de la configuración está generalmente actualizada. La planeación e implementación de la administración de cambios de TI se está volviendo más integrada con cambios en los procesos de negocios, para asegurar ese entrenamiento, se resuelven cambios organizativos y problemas de continuidad de negocio. Hay mayor coordinación entre la administración de cambios de TI y el rediseño del proceso de negocios.</td></tr>
</table>

MODELO DE MEJORES PRACTICAS - COBIT

<table>
<tr><td colspan="3">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="4">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 2/2</td></tr>
<tr><td colspan="5">MODELO DE MADUREZ</td></tr>
<tr><td colspan="3">DOMINIO: ADQUISICIÓN E IMPLEMENTACIÓN</td><td colspan="2">AI6.- Administrar Cambios</td></tr>
<tr><td colspan="5">OBJETIVO DE CONTROL</td></tr>
<tr><td colspan="5">El control sobre el proceso de TI Administrar Cambios de TI con el objetivo del negocio de minimizar la probabilidad de interrupción, alteraciones no autorizadas y errores</td></tr>
<tr><td colspan="2">Estado Actual :</td><td></td><td>Estado Proyectado:</td><td></td></tr>
<tr><td>5</td><td colspan="4">Optimizado El proceso de administración de cambios es revisado y actualizado regularmente para mantener en línea con las mejores prácticas. La información de configuración está automatizada y provee control de versiones. La distribución de software es automatizada y se cuenta con capacidades de monitoreo a distancia. La administración de configuración y liberación y rastreo de cambios es sofisticado e incluye herramientas para detectar software no autorizado y sin licencia. La administración de cambios de TI está integrada con la administración de cambios del negocio para asegurar que TI sea un posibilitador para aumentar la productividad y crear nuevas oportunidades de negocios para la organización.</td></tr>
</table>

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 1/2</td></tr>
<tr><td colspan="4">MODELO DE MADUREZ</td></tr>
<tr><td colspan="2">DOMINIO: ENTREGA Y SOPORTE</td><td colspan="2">DS4 .- Asegurar el Servicio Continuo</td></tr>
<tr><td colspan="4">OBJETIVO DE CONTROL</td></tr>
<tr><td colspan="4">El control sobre el proceso de TI Administrar Cambios de TI con el objetivo del negocio de minimizar la probabilidad de interrupción, alteraciones no autorizadas y errores</td></tr>
<tr><td>Estado Actual :</td><td>2</td><td>Estado Proyectado:3</td><td></td></tr>
<tr><td colspan="4">CRITERIOS DE CALIFICACIÓN</td></tr>
<tr><td>0</td><td colspan="3">Inexistente. No hay entendimiento de los riesgos, vulnerabilidades y amenazas de las operaciones de TI o del impacto de la pérdida de los servicios de TI para el negocio. La continuidad del servicio no es considerada como que necesita atención de la administración.</td></tr>
<tr><td>1</td><td colspan="3">Inicial /Ad hoc Las responsabilidades de servicio continuo son informales, con autoridad limitada. La administración se está volviendo conciente de los riesgos relacionados con el servicio continuo y de la necesidad de éste. El enfoque es sobre la función de TI, en vez de ser sobre la función de negocio. Los usuarios están implementando formas de evadirlo. La respuesta a las interrupciones mayores es reactiva e improvisada. Los cortes planeados están programados para que satisfagan las necesidades de TI, en vez de para adaptarse a los requerimientos del negocio.</td></tr>
<tr><td>2</td><td colspan="3">Repetible pero Intuitiva La responsabilidad del servicio continuo está asignada. Los enfoques del servicio continuo son fragmentados. El reporte sobre la disponibilidad del sistema es incompleto y no toma en cuenta el impacto sobre el negocio. No hay planes documentados de usuario o de continuidad, a pesar de que hay dedicación a la disponibilidad de servicio continuo y que se conocen sus principios rectores. Existe un inventario razonablemente confiable de sistemas críticos y componentes. Está surgiendo la estandarización de prácticas de servicio continuo y el monitoreo del proceso, pero el éxito se basa en las personas.</td></tr>
<tr><td>3</td><td colspan="3">Proceso Definido La obligación de reportar no es ambigua y las responsabilidades de planificar y probar el servicio continuo están claramente definidas y asignadas. Los planes están documentados y se basan en la importancia del sistema y en el impacto sobre el negocio. Hay un reporte periódico de prueba de servicio continuo. Las personas toman la iniciativa para seguir las normas y recibir entrenamiento. La administración comunica consistentemente la necesidad de servicio continuo. Los componentes de alta disponibilidad y la redundancia de sistema se están aplicando de manera fragmentada. Se mantiene rigurosamente un inventario de sistemas críticos y componentes.</td></tr>
</table>

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 2/2</td></tr>
<tr><td colspan="4">MODELO DE MADUREZ</td></tr>
<tr><td colspan="2">DOMINIO: ENTREGA Y SOPORTE</td><td colspan="2">DS4 .- Asegurar el Servicio Continuo</td></tr>
<tr><td colspan="4">OBJETIVO DE CONTROL</td></tr>
<tr><td colspan="4">El control sobre el proceso de TI Administrar Cambios de TI con el objetivo del negocio de minimizar la probabilidad de interrupción, alteraciones no autorizadas y errores</td></tr>
<tr><td>Estado Actual :</td><td></td><td>Estado Proyectado:</td><td></td></tr>
<tr><td colspan="4">CRITERIOS DE CALIFICACIÓN</td></tr>
<tr><td>4</td><td colspan="3">Administrado y Medible Se hacen cumplir las responsabilidades y las normas para el servicio continuo. La responsabilidad de mantener el plan de servicio continuo está asignada. Las actividades de mantenimiento toman en cuenta el entorno cambiante del negocio, los resultados de pruebas de servicio continuo y las mejores prácticas internas. Se están recopilando, analizando, reportando y ejecutando datos estructurados sobre el servicio continuo. Se provee entrenamiento para los procesos de servicio continuo. Las prácticas de redundancia de sistema, que incluyen el uso de componentes de alta disponibilidad, están siendo implementadas de manera consistente. Las prácticas de redundancia y la planeación de servicio continuo se influyen mutuamente. Los incidentes de falta de continuidad son clasificados y el paso cada vez mayor de escala para cada uno es bien conocido para todos los que están involucrados.</td></tr>
<tr><td>5</td><td colspan="3">Optimizado Los procesos integrados de servicio continuo son proactivos, se ajustas solos, son automatizados y auto analíticos y toman en cuenta puntos de referencia y las mejores prácticas externas. Los planes de servicio continuo y los planes de continuidad del negocio están integrados, alineados y son mantenidos de manera rutinaria. La compra de las necesidades de servicio continuo está asegurada por los vendedores y los principales proveedores. Se lleva a cabo la comprobación global y los resultados de las pruebas son utilizados como parte del proceso de mantenimiento. La efectividad del costo del servicio continuo está optimizada a través de la innovación y de la integración. La recopilación y el análisis de datos se usa para identificar oportunidades de mejoramiento. Las prácticas de redundancia y la planeación del servicio continuo están totalmente alineadas. La administración no permite puntos únicos de falla y provee soporte para su solución. Las prácticas de escalamiento son entendidas y cumplidas plenamente.</td></tr>
</table>

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 1/2</td></tr>
<tr><td colspan="4">MODELO DE MADUREZ</td></tr>
<tr><td colspan="2">DOMINIO: ENTREGA Y SOPORTE</td><td colspan="2">DS5 .- Garantizar la Seguridad de los Sistemas</td></tr>
<tr><td colspan="4">OBJETIVO DE CONTROL</td></tr>
<tr><td colspan="4">El control sobre el proceso de TI Garantizar la Seguridad de los Sistemas de TI con el objetivo del negocio de salvaguardar la información contra el uso, revelación o modificación no autorizada, daño o pérdida.</td></tr>
<tr><td>Estado Actual :</td><td>1</td><td>Estado Proyectado:</td><td>3</td></tr>
<tr><td colspan="4">CRITERIOS DE CALIFICACIÓN</td></tr>
<tr><td>0</td><td colspan="3">Inexistente. La organización no reconoce la necesidad de la seguridad de TI. Las responsabilidades y las obligaciones de reportar no están asignadas para asegurar la seguridad. No están implementadas medidas que soporten la administración de la seguridad de TI. No hay ningún reporte de seguridad de TI y ningún proceso de respuesta de las violaciones de seguridad de TI. Hay una carencia total de un proceso reconocible de administración de seguridad de sistemas.</td></tr>
<tr><td>1</td><td colspan="3">Inicial /Ad hoc La organización reconoce la necesidad de la seguridad de TI, pero la conciencia de la seguridad depende de la persona. La seguridad de TI está resuelta de manera reactiva y no se mide. Las violaciones de seguridad de TI invocan respuestas de “señalamiento” si se detectan, porque las responsabilidades no están claras. Las respuestas a las violaciones de seguridad de TI son impredecibles.</td></tr>
<tr><td>2</td><td colspan="3">Repetible pero Intuitiva Las responsabilidades y obligaciones de la seguridad de TI están asignadas a un coordinador de seguridad de TI que no tiene autoridad de administración. La conciencia de seguridad es fragmentada y limitada. La información de seguridad de TI es generada, pero no es analizada. Las soluciones de seguridad tienden a responder de manera reactiva a los incidentes de seguridad de TI y adoptando propuestas de terceros, sin resolver las necesidades específicas de la organización. Se están desarrollando políticas de seguridad, pero aún se siguen usando habilidades y herramientas inadecuadas. El reporte de seguridad de TI es incompleto, engañoso y no es pertinente.</td></tr>
<tr><td>3</td><td colspan="3">Proceso Definido Existe conciencia de la seguridad y la misma es promovida por la administración. Se han estandarizado y formalizados reportes de conocimientos de la seguridad. Los procedimientos de seguridad de TI están definidos y encajan en una estructura para políticas y procedimientos de seguridad. Las responsabilidades de seguridad de TI están asignadas, pero no se hacen cumplir de manera consistente. Existe un plan de seguridad de TI, que impulsa el análisis del riesgo y soluciones de seguridad. El reporte de seguridad de TI está concentrado en TI, en lugar de concentrarse en el negocio. Se realizan pruebas Ad hoc de intrusión.</td></tr>
</table>

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 2/2</td></tr>
<tr><td colspan="4">MODELO DE MADUREZ</td></tr>
<tr><td colspan="2">DOMINIO: ENTREGA Y SOPORTE</td><td colspan="2">DS5 .- Garantizar la Seguridad de los Sistemas</td></tr>
<tr><td colspan="4">OBJETIVO DE CONTROL</td></tr>
<tr><td colspan="4">El control sobre el proceso de TI Garantizar la Seguridad de los Sistemas de TI con el objetivo del negocio de salvaguardar la información contra el uso, revelación o modificación no autorizada, daño o pérdida.</td></tr>
<tr><td>Estado Actual :</td><td></td><td>Estado Proyectado:</td><td></td></tr>
<tr><td colspan="4">CRITERIOS DE CALIFICACIÓN</td></tr>
<tr><td>4</td><td colspan="3">Administrado y Medible Las responsabilidades de la seguridad de TI están claramente asignadas, administradas y se hacen cumplir. El análisis de riesgo e impacto de seguridad se lleva a cabo de manera consistente. Las políticas y prácticas de seguridad son completadas con bases específicas de seguridad. Los reportes de conocimiento de seguridad se han vuelto obligatorios. La identificación, autenticación y autorización de usuario se está estandarizando. Se está estableciendo la certificación de seguridad del personal. La prueba de intrusión es un proceso estándar y formalizado que conduce a mejoras. El análisis costo / beneficio, que soporta la implementación de medidas de seguridad, es cada vez más utilizado. Los procesos de seguridad de TI son coordinados con la función general de seguridad de la organización. El reporte de seguridad de TI está vinculado con los objetivos del negocio.</td></tr>
<tr><td>5</td><td colspan="3">Optimizado La seguridad de TI es una responsabilidad conjunta del negocio y de la administración de TI y está integrada con objetivos de seguridad corporativa del negocio. Los requisitos de seguridad de TI están claramente definidos, optimizados e incluidos en un plan verificado de seguridad. Las funciones de seguridad están integradas con aplicaciones en la etapa de diseño y se les puede pedir a los usuarios finales que rindan cuenta de la seguridad a la administración. El reporte de seguridad de TI provee un aviso anticipado del riesgo cambiante y emergente, usando métodos activos automatizados de monitoreo para los sistemas críticos. Los incidentes son prontamente resueltos con procedimientos formalizados de respuesta a incidentes soportados por herramientas automatizadas. Las evaluaciones periódicas de seguridad evalúan la efectividad de la implementación del plan de seguridad. Se recoge y analiza sistemáticamente la información sobre nuevas amenazas y vulnerabilidades, y se comunican e implementan prontamente los controles adecuados de mitigación. La prueba de intrusión, análisis de las causas originarias de los incidentes de seguridad y la identificación proactiva del riesgo es la base para el mejoramiento continuo. Los procesos y las tecnologías de seguridad están integrados en toda la organización.</td></tr>
</table>

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 1/2</td></tr>
<tr><td colspan="4">MODELO DE MADUREZ</td></tr>
<tr><td colspan="2">DOMINIO: ENTREGA Y SOPORTE</td><td colspan="2">DS11 .- Administrar los Datos</td></tr>
<tr><td colspan="4">OBJETIVO DE CONTROL</td></tr>
<tr><td colspan="4">El control sobre el proceso de TI Administrar Cambios de TI con el objetivo del negocio de minimizar la probabilidad de interrupción, alteraciones no autorizadas y errores</td></tr>
<tr><td>Estado Actual :</td><td>2</td><td>Estado Proyectado:</td><td>4</td></tr>
<tr><td colspan="4">CRITERIOS DE CALIFICACIÓN</td></tr>
<tr><td>0</td><td colspan="3">Inexistente. No se reconocen los datos como un recurso y un activo corporativo. No hay propiedad asignada de datos ni responsabilidad individual de la integridad y confiabilidad de los datos. La calidad y seguridad de los datos son deficientes o inexistentes.</td></tr>
<tr><td>1</td><td colspan="3">Inicial /Ad hoc La organización reconoce una necesidad de datos exactos. Algunos métodos son desarrollados a nivel individual para prevenir y detectar el ingreso, procesamiento y errores en la salida de los datos. El proceso de identificación y corrección de errores depende de las actividades manuales de la persona, y las reglas y requerimientos no son transmitidos a medida que se llevan a cabo movimientos y cambios de personal. La administración asume que los datos son exactos porque una computadora está involucrada en el proceso. La integridad y seguridad de los datos no son requerimientos de administración y, si existe la seguridad, ésta está administrada por la función de servicios de información.</td></tr>
<tr><td>2</td><td colspan="3">Repetible pero Intuitivo La conciencia de la necesidad de la exactitud de los datos y de mantener la integridad prevalece en toda la organización. La propiedad de los datos comienza a tener lugar, pero a nivel de un departamento o grupo. Las reglas y requerimientos son documentados por personas clave y no son consistentes en toda la organización y plataformas. Los datos están en custodia de la función de los servicios de información y las reglas y definiciones están impulsadas por los requerimientos de TI. La seguridad e integridad de los datos son primariamente responsabilidades de la función de los servicios de información con una participación departamental menor.</td></tr>
<tr><td>3</td><td colspan="3">Proceso Definido La necesidad de integridad de los datos dentro y en toda la organización es entendida y aceptada. Las normas de ingreso, procesamiento y salida de datos han sido formalizadas y se hacen cumplir. El proceso de identificación y corrección de errores es automatizado. La propiedad de los datos es asignada, y la integridad y seguridad son controladas por el responsable. Se utilizan técnicas automatizadas para prevenir y detectar errores e inconsistencias. Las definiciones, reglas y requerimientos de datos están claramente documentados y son mantenidos por una función de administración de base de datos. Los datos se vuelven consistentes en todas las plataformas y a través de toda la organización. La función de los servicios de información tiene un rol de custodio, mientras que el control de integridad de datos pasa al propietario de los datos. La administración se basa en los reportes y análisis para las decisiones y la planeación futuras.</td></tr>
</table>

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 2/2</td></tr>
<tr><td colspan="4">MODELO DE MADUREZ</td></tr>
<tr><td colspan="2">DOMINIO: ENTREGA Y SOPORTE</td><td colspan="2">DS11 .- Administrar los Datos</td></tr>
<tr><td colspan="4">OBJETIVO DE CONTROL</td></tr>
<tr><td colspan="4">El control sobre el proceso de TI Administrar Cambios de TI con el objetivo del negocio de minimizar la probabilidad de interrupción, alteraciones no autorizadas y errores</td></tr>
<tr><td>Estado Actual :</td><td></td><td>Estado Proyectado:</td><td></td></tr>
<tr><td colspan="4">CRITERIOS DE CALIFICACIÓN</td></tr>
<tr><td>4</td><td colspan="3">Administrado y Medible Los datos son definidos como un recurso y un activo corporativo, a medida que la administración exige más soporte de decisiones y más reporte de rentabilidad. La responsabilidad por la calidad de datos está claramente definida, asignada y comunicada dentro de la organización. Los métodos estandarizados están documentados, mantenidos, y usados para controlar la calidad de los datos, se hacen cumplir las reglas y los datos son consistentes en todas las plataformas y unidades de negocio. La calidad de los datos es medida y la satisfacción del cliente respecto a la información es monitoreada. El reporte de administración asume un valor estratégico para asesorar clientes, tendencias y evaluaciones de productos. La integridad de los datos se vuelve un factor significativo, con la seguridad de datos reconocida como un requerimiento de control. Se ha establecido una función formal de administración de datos a nivel de toda la organización, con los recursos y la autoridad para hacer cumplir la estandarización de datos.</td></tr>
<tr><td>5</td><td colspan="3">Optimizado La administración de datos es un proceso maduro, integrado y de funcionamiento cruzado que tiene una meta claramente definida y bien entendida de entregar información de calidad al usuario, con criterios claramente definidos de integridad, disponibilidad y confiabilidad. La organización maneja activamente datos, información y conocimientos como los recursos y los activos corporativos, con el objetivo de maximizar el valor del negocio. La cultura corporativa hace énfasis en la importancia de datos de alta calidad que necesitan ser protegidos y tratados como un componente clave de capital intelectual. La propiedad de datos es una responsabilidad estratégica con todos los requerimientos, reglas, reglamentaciones y consideraciones claramente documentados, mantenidos y comunicados.</td></tr>
</table>

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 1/2</td></tr>
<tr><td colspan="4">MODELO DE MADUREZ</td></tr>
<tr><td colspan="2">DOMINIO : Entrega y Soporte</td><td colspan="2">DS12 .- Administrar Instalaciones</td></tr>
<tr><td colspan="4">OBJETIVO DE CONTROL</td></tr>
<tr><td colspan="4">Control sobre el proceso de TI Administrar Instalaciones con el objetivo del negocio de proveer un entorno físico adecuado que proteja el equipo y la gente de TI contra los riesgos naturales y provocados por el hombre.</td></tr>
<tr><td>Estado Actual :</td><td>2</td><td>Estado Proyectado:</td><td>4</td></tr>
<tr><td colspan="4">CRITERIOS DE CALIFICACIÓN</td></tr>
<tr><td>0</td><td colspan="3">Inexistente. No hay conciencia de la necesidad de proteger las Instalaciones o la inversión en los recursos de computación. Los factores ambientales, incluyendo la protección contra incendios, el polvo, la energía y el calor y la humedad excesivos, no son monitoreados ni controlados.</td></tr>
<tr><td>1</td><td colspan="3">Inicial /Ad hoc La organización ha reconocido un requerimiento del negocio de proveer un entorno físico adecuado que proteja los recursos y el personal de los riesgos naturales y provocados por el hombre. No existen procedimientos estándar y la administración de Instalaciones y equipo depende de las habilidades y capacidades de las personas clave. No se revisa el mantenimiento y la gente se mueve dentro de las Instalaciones sin restricción. La administración no monitorea los controles ambientales de la instalación ni el movimiento de personal.</td></tr>
<tr><td>2</td><td colspan="3">Repetible pero intuitivo La conciencia de la necesidad de proteger y de controlar el entorno físico de computación es reconocida y evidente en la asignación de los presupuestos y de otros recursos. Los controles ambientales son implementados y monitoreados por el personal de operaciones. La seguridad física es un proceso informal, impulsado por un pequeño grupo de empleados que tienen un alto nivel de preocupación sobre la seguridad de las Instalaciones físicas. Los procedimientos de mantenimiento de las Instalaciones no están bien documentados y se basan en las mejores prácticas de unas pocas personas. Las metas de la seguridad física no se basan en ningún estándar formal y la administración no asegura que se logren los objetivos de seguridad.</td></tr>
<tr><td>3</td><td colspan="3">Proceso Definido La necesidad de mantener un entorno controlado de computación es entendida y aceptada dentro de la organización. Los controles ambientales, de mantenimiento preventivo y de seguridad física son rubros del presupuesto aprobados y la administración les hace seguimiento. Se aplican restricciones de acceso, permitiéndose el acceso a las Instalaciones de computación sólo al personal aprobado. Los visitantes son registrados y a veces escoltados, dependiendo del personal responsable. Las Instalaciones físicas tienen perfil bajo y no se pueden identificar fácilmente. Las autoridades civiles monitorean el cumplimiento de las reglamentaciones sanitarias y de seguridad. Los riesgos están asegurados, pero no se hace esfuerzo alguno para optimizar los costos de seguros.</td></tr>
</table>

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 2/2</td></tr>
<tr><td colspan="4">MODELO DE MADUREZ</td></tr>
<tr><td colspan="2">DOMINIO : Entrega y Soporte</td><td colspan="2">DS12 .- Administrar Instalaciones</td></tr>
<tr><td colspan="4">OBJETIVO DE CONTROL</td></tr>
<tr><td colspan="4">Control sobre el proceso de TI Administrar Instalaciones con el objetivo del negocio de proveer un entorno físico adecuado que proteja el equipo y la gente de TI contra los riesgos naturales y provocados por el hombre.</td></tr>
<tr><td>Estado Actual :</td><td></td><td>Estado Proyectado:</td><td></td></tr>
<tr><td colspan="4">CRITERIOS DE CALIFICACIÓN</td></tr>
<tr><td>4</td><td colspan="3">Administrado y Medible La necesidad de mantener un entorno controlado de computación es entendida totalmente, como es evidente en la estructura organizacional y en la asignación de presupuesto. Los requerimientos ambientales y de seguridad física están documentados y el acceso está estrictamente controlado y monitoreado. La responsabilidad y la propiedad han sido establecidas y comunicadas. El personal de las Instalaciones ha sido totalmente entrenado en situaciones de emergencia, así como también en prácticas sanitarias y de seguridad. Están estandarizados los mecanismos de control para restringir el acceso a las Instalaciones y para resolver factores ambientales y de seguridad. La administración monitorea la efectividad de los controles y el cumplimiento de las normas establecidas. La recuperación de los recursos de computación está incorporada al proceso corporativo de administración de riesgos. Están desarrollados planes para toda la organización, se llevan a cabo pruebas regulares e integradas y las lecciones aprendidas son incorporadas en las revisiones de los planes. La información integrada se usa para optimizar la cobertura de seguros y los costos relacionados.</td></tr>
<tr><td>5</td><td colspan="3">Optimizado Hay un plan a largo plazo para las Instalaciones que se requiere que soporten el entorno de computación de la organización. Las normas están definidas para todas las Instalaciones, abarcando la selección del sitio, la construcción, custodia, seguridad de personal, sistemas mecánico y eléctrico, protección contra incendio, rayo e inundación. Todas las Instalaciones son inventariadas y clasificadas en conformidad con el proceso de administración de riesgos de la organización en progreso. El acceso está estrictamente controlado y se basa en la necesidad para el trabajo, es monitoreado constantemente y los visitantes son escoltados en todo momento. El entorno es monitoreado y controlado por medio de equipo especializado y las salas de equipos se vuelven automatizadas. Los programas de mantenimiento preventivo hacen cumplir estrictamente los programas y se aplican pruebas regulares a los equipos sensitivos. La estrategia y normas de las Instalaciones están en correspondencia con los objetivos de disponibilidad de servicios de TI y están integradas con la planeación de la continuidad del negocio y con la administración de crisis. La administración revisa y optimiza las Instalaciones constantemente, capitalizando sobre las oportunidades de mejorar la contribución del negocio.</td></tr>
</table>

Enfoque del Modelo de Madurez

El enfoque de los Modelos de Madurez para el control sobre los procesos de TI consiste en desarrollar un método de asignación de puntos para que una organización pueda calificarse desde Inexistente hasta optimizada (de 0 a 5). Este planteamiento se basa en el Modelo de Madurez que el Software Engineering Institute definió para la madurez de la capacidad de desarrollo de software. Cualquiera sea el modelo, las escalas no deben estar demasiado simplificadas, lo que haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable.

En contraste, uno debe concentrarse en los niveles de madurez basándose en un conjunto de condiciones que pueden ser satisfechas de una forma que no sea ambigua. En comparación con los niveles desarrollados para cada uno de los 34 procesos de TI de COBIT, la administración puede mapear:

- La situación actual de la organización—dónde está la organización actualmente
- La estrategia de la organización para mejoramiento—dónde quiere estar la organización

RESUMEN GERENCIAL DEL MODELO DE MADUREZ PARA LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN

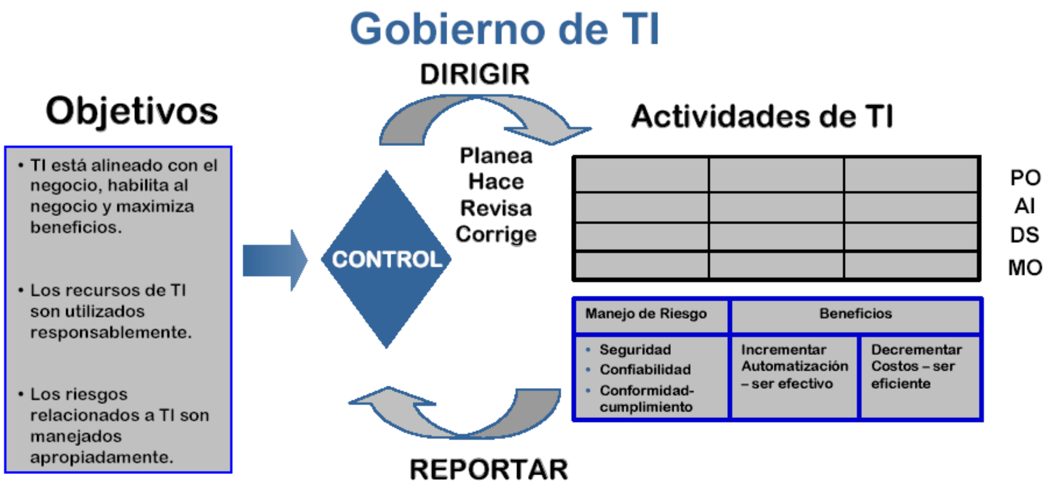
		Inexistente	Inicial /Ad Hoc	Repetible pero Intuitivo	Proceso Definido	Administrado y Medible	Optimizado
		0	1	2	3	4	5
PO9	Evaluar los Riesgos						
PO11	Administrar Calidad						
AI6	Administrar Cambios						
DS4	Asegurar el Servicio Continuo						
DS5	Garantizar la Seguridad de los Sistemas						
DS11	Administrar los Datos						
DS12	Administrar Instalaciones						

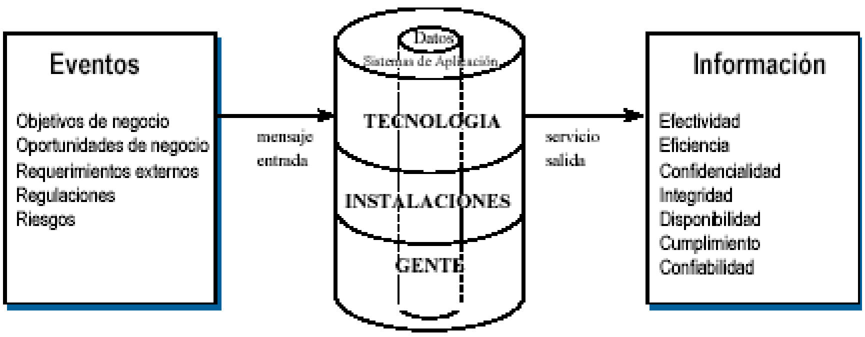
LEYENDA PARA LOS SÍMBOLOS USADOS		LEYENDA PARA LAS CLASIFICACIONES USADAS	
	Situación actual de la empresa	0 Inexistente 1 Inicial 2 Repetible 3 Definida 4 Administrada 5 Optimizada	Los procesos de administración no se aplican en absoluto Los procesos son ad hoc y desorganizados Los procesos siguen un patrón regular Los procesos son documentados y comunicados Los procesos son monitoreados y medidos Las mejores prácticas son seguidas y automatizadas
	Estrategia de la Empresa		

7 EVALUACIÓN DE RIESGO DE LOS 105 OBJETIVOS DE CONTROL

7.1 Administración de Riesgos

Para asegurar que la Gerencia alcance los objetivos de negocios, ésta debe dirigir y administrar las actividades de TI para alcanzar un balance efectivo entre el manejo de riesgos y los beneficios encontrados. Para cumplir esto, la Gerencia necesita identificar las actividades mas importantes que deben ser desarrolladas, midiendo el progreso hacia el cumplimiento de las metas y determinando que tan bien se están desarrollando los procesos de TI. Aun mas, necesita tener la habilidad de avaluar el nivel de madurez de la organización contra las mejores practicas industriales y los modelos internacionales.





Definición.-

Es un **proceso interactivo** e **iterativo** basado en el conocimiento, evaluación y manejo de los riesgos y sus impactos, con el propósito de mejorar la toma de decisiones organizacionales.

Aplicable a cualquier situación donde un resultado no deseado o inesperado pueda ser significativo o donde se identifiquen oportunidades.

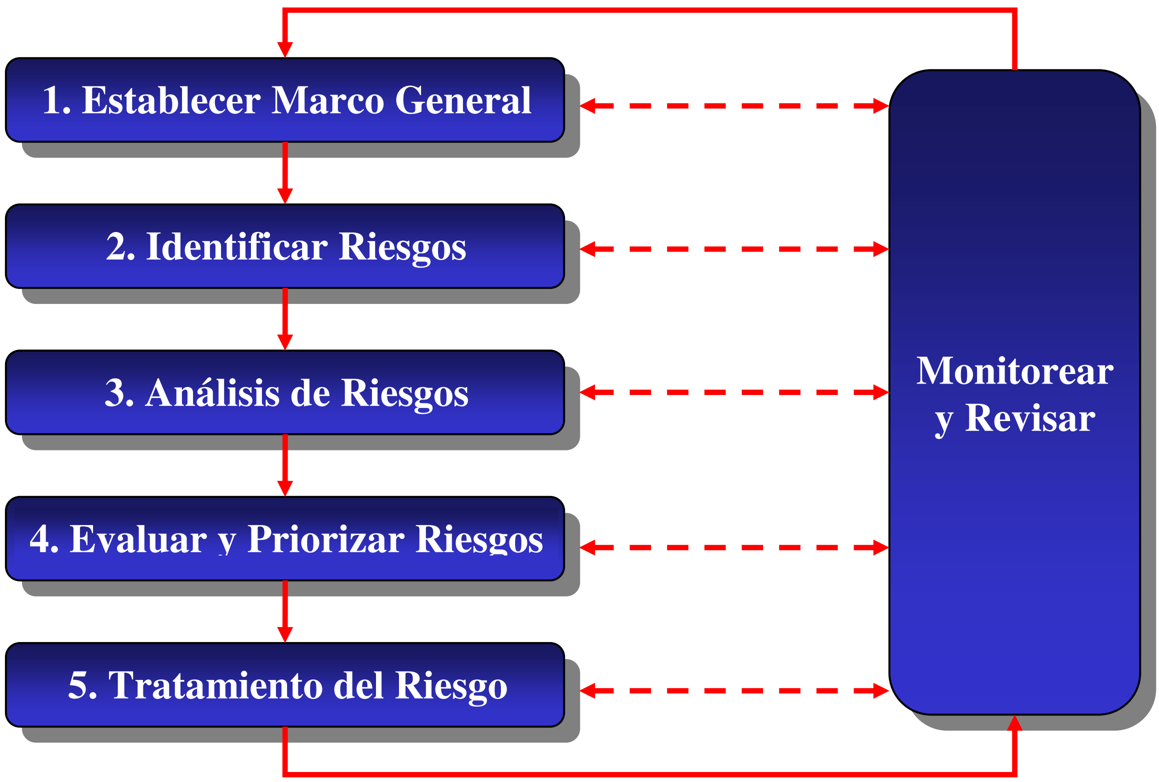
Beneficios para la Organización

- Facilita el logro de los objetivos de la organización.
- Hace a la organización más segura y consciente de sus riesgos.
- Mejoramiento continúo del Sistema de Control Interno.
- Optimiza la asignación de recursos.
- Aprovechamiento de oportunidades de negocio.
- Fortalece la cultura de autocontrol.
- Mayor estabilidad ante cambios del entorno.

Beneficios para el Dpto. de Auditoría

- Soporta el logro de los objetivos de la auditoría.
- Estandarización en el método de trabajo.
- Integración del concepto de control en las políticas organizacionales.
- Mayor efectividad en la planeación general de Auditoría.
- Evaluaciones enfocadas en riesgos.
- Mayor cobertura de la administración de riesgos.
- Auditorías más efectivas y con mayor valor agregado.

7.2 Proceso de administración de Riesgos



7.2.1 Establecer Marco General

Ecuacolor es una marca reconocida, posee una presencia bastante fuerte en el mercado fotográfico a nivel nacional, con más de 100 fototiendas. Ha llegado a poseer el 70% de participación del mercado.

- Es parte de un grupo económico conformado por Comandato, OndaPositiva, TecniPrint.
- Mucha de la infraestructura tecnológica es compartida por el Grupo Corporativo.
- Existen Niveles Gerenciales que cumplen sus funciones de manera Corporativo.

El mercado fotográfico en el Ecuador esta cambiando, el cambio se esta dando hacia el revelado digital, lo que motiva que el mercado de revelado tradicional se vea disminuido, afectando a los ingresos de la institución.

Para contrarrestar este efecto, la institución ha diseñado nuevas estrategias y desarrollado nuevas líneas de negocio.

Entre las estrategias de mas alto impacto están:

- Venta a Crédito, lo que debe incrementar la venta de Cámaras Digitales y otros productos de la línea Profesional.
- Se ha logrado obtener la representación exclusiva de los productos Maxell en todo el territorio nacional, de tal manera que se diversifican los ingresos que tiene la institución actualmente.
- Promociones para impulsar el revelado digital.
- Alianzas estratégicas con empresas nacionales para promociones cruzadas.
- Adquisición de Equipos de revelado digital PictureMaker.

Para lograr alcanzar los objetivos estratégicos definidos existen adquisiciones de tecnología que tienen una incidencia directa en el plan estratégicos de negocio.

- Adquisición de nuevo sistema de punto de ventas que cumpla los requerimientos de ley acorde a las necesidades y expectativas del negocio.
- Implementación de interconexión entre las principales tiendas a nivel nacional con la casa matriz.
- **Administración de la tecnología actual que soporta los procesos del negocio. Siendo este ultimo uno de los pilares fundamentales en la consecución de las metas trazadas por la organización.**

Los costos de estos proyectos son bastante significativos dentro de los resultados de la empresa, por eso razón la evaluación y adquisición de la tecnología antes mencionada debe ser llevada a cabo de la mejor manera posible.

Ecuacolor esta enfocado en 2 segmentos, la venta a través de su cadena de retail y la venta a distribuidores.

Los principales competidores de Ecuacolor en el segmento de retail, son Konica, Fuji, Fybeca, otros quedan servicio de revelado. En lo que respecta a la distribución de Kodak y Maxell, es la misma que la de la marca a nivel internacional.

Actualmente la marca Ecuacolor esta catalogada como la numero uno en cuanto al revelado fotográfico y apunta a mantener esta posición. Ecuacolor siempre esta buscando la manera de incrementar su volumen de ventas, lanzando promociones. Sin embargo las ventas están disminuyendo debido a cambios que están surgiendo en el revelado tradicional, siendo esta la principal fuente de sus ingresos.

7.2.2 Identificar Riesgos

Los riesgos son amenazas que podrían explotar las vulnerabilidades de nuestra infraestructura tecnología ocasionando daños o pérdidas a los activos, de tal manera que habría dificultad en conseguir los Objetivos Empresariales.

Establecer un marco específico de administración de riesgos.

Entender la actividad o parte de la organización para la cual se aplicará el proceso de administración de riesgos.

Basándonos en la metodología COBIT, en donde se identifican 34 procesos que rigen la Administración y Control de tecnología de información y como estos son impactados principalmente por las características de seguridad de la información (Confidencialidad, Disponibilidad, e Integridad) se han seleccionado los procesos que a continuación se detallan.

			confidencialidad	**Integridad**	**Disponibilidad**
DOMINIO	PROCESO		Criterios de información		
Planeación y Organización	PO9	Evaluar riesgos	P	P	P
	PO11	Administrar Calidad		P	
Adquisición e Instalación	AI6	Administrar cambios		P	P
Entrega de Servicios	DS4	Asegurar continuidad del servicio			P
	DS5	Garantizar la seguridad de sistemas	P	P	
	DS11	Administrar la información		P	
	DS12	Administrar las instalaciones		P	P

Criterios de evaluación de riesgos.-

Definir e identificar los criterios de análisis y el nivel de aceptación de los riesgos

Criterios de análisis.-

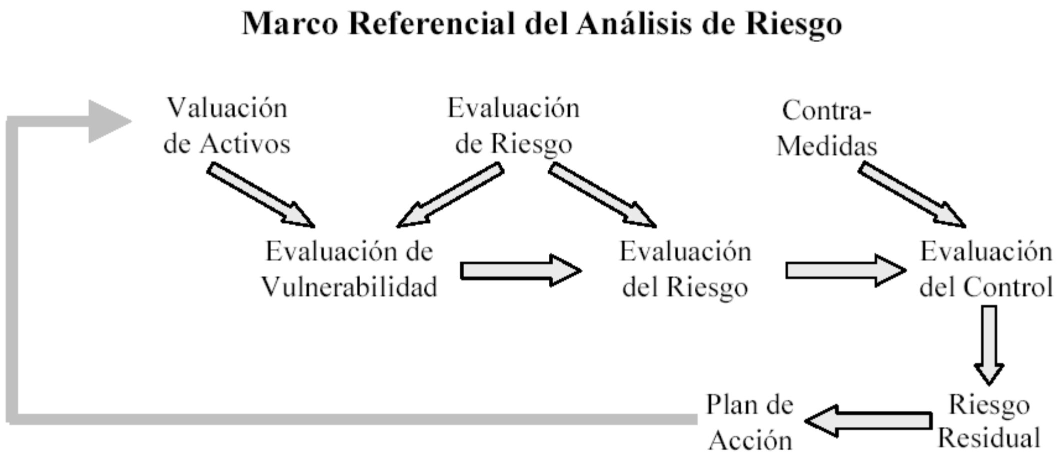
Criterio	Probabilidad de Ocurrencia	Impacto
ALTO	9	10
MEDIO ALTO	7	8
MEDIO	5	6
MEDIO BAJO	3	4
BAJO	1	2

Nivel de Aceptación de Riesgo.-

Riesgo = Probabilidad de Ocurrencia * Impacto

Nivel de Aceptación de Riesgo		
BAJO **1 - 30**	**MEDIO** **31-60**	ALTO 61 – 90

7.2.3 Análisis de Riesgos



El modelo comienza a partir de la valoración de los activos, que dentro del *Marco Referencial* de COBIT consiste en la información que tiene los criterios requeridos para ayudar a lograr los objetivos del negocio (incluyendo todos los recursos necesarios para producir dicha información). El siguiente paso es el análisis de vulnerabilidad† que trata de la importancia de los criterios de información dentro del proceso bajo revisión, por ejemplo, si un proceso del negocio es vulnerable a la pérdida de integridad, entonces se requieren medidas específicas. Luego se tratan las amenazas, esto es, aquello que puede provocar una vulnerabilidad. La probabilidad de la amenaza, el grado de vulnerabilidad y la severidad del impacto se combinan para concluir acerca de la evaluación del riesgo. Esto es seguido por la selección de contramedidas (controles) y una evaluación de su eficacia, que también identifica el riesgo residual. La conclusión es un plan de acción después del cual el ciclo puede comenzar nuevamente.

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
PO9	Evaluar Riesgo	Soportar las decisiones administrativas a través del logro de los objetivos de TI y responder a las amenazas reduciendo la complejidad, Incrementando la objetividad e identificando factores de decisión importante				
9.1	Evaluación de Riesgos del Negocio	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 con participación multidisciplinaria. La Administración deberá asegurar que se realicen reevaluaciones y que la información sobre evaluación de riesgos sea actualizada como resultado de auditorías, inspecciones e incidentes identificados.	MEDIO-ALTO	MEDIO-ALTO	56	
9.2	Enfoque de Evaluación de Riesgos	La Gerencia deberá establecer un enfoque general para la evaluación de riesgos que defina el alcance y los límites, la metodología a ser adoptada para las evaluaciones de riesgos, las responsabilidades y las habilidades requeridas. La Gerencia debe adelantar la identificación de soluciones para la mitigación de riesgos e involucrarse en la identificación de vulnerabilidades. Especialistas de seguridad deben realizar identificación de amenazas y especialistas de TI deben dirigir la selección de controles. La calidad de las evaluaciones de riesgos deberá estar asegurada por un método estructurado y por asesores expertos en riesgos.	MEDIO-ALTO	MEDIO-ALTO	56	

OBJETIVOS DE CONTROL	OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN

PO9	Evaluar Riesgo	Soportar las decisiones administrativas a través del logro de los objetivos de TI y responder a las amenazas reduciendo la complejidad, Incrementando la objetividad e identificando factores de decisión importante				
9.3	Identificación de Riesgos	La evaluación de riesgos deberá enfocarse al examen de los elementos esenciales de riesgo y las relaciones causa/efecto entre ellos. Los elementos esenciales de riesgo incluyen activos tangibles e intangibles, valor de los activos, amenazas, vulnerabilidades, protecciones, consecuencias y probabilidad de amenaza. El proceso de identificación de riesgos debe incluir una clasificación cualitativa y, donde sea apropiado, clasificación cuantitativa de riesgos debe obtener insumos de las tormentas de ideas de la Gerencia, de planeación estratégica, auditorías anteriores y otros análisis. El análisis de riesgos debe considerar el negocio, regulaciones, aspectos legales, tecnología, comercio entre socios y riesgos del recurso humano.	MEDIO	MEDIO	30	
9.4	Medición de Riesgos	El enfoque de la evaluación de riesgos deberá asegurar que la información del análisis de la identificación de riesgos genere como resultado una medida cuantitativa y/o cualitativa del riesgo al cual está expuesta el área examinada. Asimismo, deberá evaluarse la capacidad de aceptación de riesgos de la organización.	MEDIO-ALTO	MEDIO	42	
9.5	Plan de Acción contra Riesgos	El enfoque de evaluación de riesgos deberá proporcionar la definición de un plan de acción contra riesgos para asegurar que el costo–efectividad de los controles y las medidas de seguridad mitiguen los riesgos en forma continua. El plan de acción contra los riesgos debe identificar la estrategia de riesgos en términos de evitar, mitigar o aceptar el riesgo.	MEDIO-ALTO	MEDIO-ALTO	56	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
PO9	Evaluar Riesgo	Soportar las decisiones administrativas a través del logro de los objetivos de TI y responder a las amenazas reduciendo la complejidad, Incrementando la objetividad e identificando factores de decisión importante				
9.6	Aceptación de Riesgos	El enfoque de la evaluación de riesgos deberá asegurar la aceptación formal del riesgo residual, dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y el costo-efectividad de la implementación de protecciones y controles. El riesgo residual deberá compensarse con una cobertura de seguro adecuada, compromisos de negociación contractual y autoaseguramiento.	MEDIO-ALTO	MEDIO	42	
9.7	Selección de Garantías o Protecciones	Mientras se logra un sistema de controles y garantías razonable, apropiado y proporcional, controles con el mas alto retorno de inversión ROI - return of investment) y aquellos que provean ganancia rápida deben recibir la primera prioridad. El sistema de control necesita además balancear las medidas de prevención, detección, corrección y recuperación. Adicionalmente, la Gerencia necesita comunicar el propósito de las medidas de control, manejar el conflicto y monitorear continuamente la efectividad de las medidas de control.	MEDIO-ALTO	MEDIO	42	
9.8	Compromiso con el Análisis de Riesgos	La Gerencia deberá motivar el análisis de riesgos como una herramienta importante para proveer información para el diseño e implementación de controles internos, en la definición del plan estratégico de tecnología de información y en los mecanismos de evaluación y monitoreo.	MEDIO	MEDIO	30	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
PO11	Administración de la calidad	Cumplir con los requerimientos del cliente de TI				
11.1	Plan General de Calidad	La alta gerencia deberá desarrollar y mantener regularmente un plan general de calidad basado en los planes organizacionales y de tecnología de información a largo plazo. El plan deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.	MEDIO-ALTO	MEDIO	42	
11.2	Enfoque de Aseguramiento de Calidad	La Gerencia deberá establecer un enfoque estándar con respecto al aseguramiento de calidad, que cubra tanto las actividades de aseguramiento de calidad generales como las específicas de un proyecto. El enfoque deberá determinar el (los) tipo(s) de actividades de aseguramiento de calidad (tales como revisiones, auditorías, inspecciones, etc.) que deben realizarse para alcanzar los objetivos del plan general de calidad. Asimismo deberá requerir una revisión específica de aseguramiento de calidad.	MEDIO-ALTO	MEDIO	42	
11.3	Planeación del Aseguramiento de Calidad	La Gerencia deberá implementar un proceso de planeación de aseguramiento de calidad para determinar el alcance y la duración de las actividades de aseguramiento de calidad.	MEDIO-ALTO	MEDIO	42	
11.4	Revisión del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares y Procedimiento s de TI	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 TI.	MEDIO-BAJO	MEDIO-ALTO	24	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
PO11	Administración de la calidad	Cumplir con los requerimientos del cliente de TI				
11.5	Metodología del Ciclo de Vida de Desarrollo de Sistemas	La alta gerencia de la organización deberá definir e implementar stándares de sistemas de información y adoptar una metodología del ciclo de vida de desarrollo de sistemas que gobierne el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información computarizados y tecnologías relacionadas. 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.	MEDIO	MEDIO	30	
11.6	Metodología del Ciclo de Vida de Desarrollo de Sistemas para Cambios Mayores a la Tecnología Actual	En el caso de requerirse cambios mayores a la tecnología actual, como en el caso de adquisición de nueva tecnología, la Gerencia deberá asegurar el cumplimiento de la metodología del ciclo de vida de desarrollo de sistemas, .	MEDIO	MEDIO	30	
11.7	Actualización de la Metodología del Ciclo de Vida de Desarrollo de Sistemas	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.	MEDIO	MEDIO	30	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
PO11	Administración de la calidad	Cumplir con los requerimientos del cliente de TI				
11.8	Coordinación y Comunicación	La Gerencia deberá establecer un proceso para asegurar la coordinación y comunicación estrecha entre los clientes de la función TI y los implementadores de sistemas. Este proceso deberá ocasionar que los métodos estructurados que utilice la metodología del ciclo de vida de desarrollo de sistemas aseguren la provisión de soluciones de tecnología de información de calidad que satisfagan las demandas de negocio. La Gerencia deberá promover una organización que se caracterice por la estrecha cooperación y comunicación a lo largo del ciclo de vida de desarrollo de sistemas.	MEDIO-BAJO	MEDIO-ALTO	24	
11.9	Marco de Referencia de Adquisición y Mantenimiento para la Infraestructura de Tecnología	Deberá establecerse un marco de referencia general referente a la adquisición y mantenimiento de la infraestructura de tecnología. Los diferentes pasos que deben ser seguidos con respecto a la infraestructura de tecnología (tales como adquisición; programación, documentación y pruebas; establecimiento de parámetros; mantenimiento y aplicación de correcciones) deberán estar regidos por y mantenerse en línea con el marco de referencia para la adquisición y mantenimiento de la infraestructura de tecnología.	MEDIO	ALTO	50	

OBJETIVOS DE CONTROL	OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN

PO11	Administración de la calidad	Cumplir con los requerimientos del cliente de TI				
11.10	Relaciones con Terceras Partes como Implementadores	La Gerencia deberá crear un proceso para asegurar las buenas relaciones de trabajo con los implementadores externos que pertenezcan a terceras partes. Dicho proceso deberá disponer que el usuario y el implementador estén de acuerdo sobre los criterios de aceptación, el manejo de cambios, los problemas durante el desarrollo, las funciones de los usuarios, las instalaciones, las herramientas, el software, los estándares y los procedimientos.	MEDIO-BAJO	MEDIO-BAJO	12	
11.11	Estándares para la Documentación de Programas	La metodología del ciclo de vida de desarrollo de sistemas deberá incorporar estándares para la documentación de programas que hayan sido comunicados y ratificados al personal interesado. La metodología deberá asegurar que la documentación creada durante el desarrollo del sistema de información o durante la modificación de los proyectos coincida con estos estándares.	MEDIO-BAJO	MEDIO-ALTO	24	
11.12	Estándares para Pruebas de Programas	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 o modificación de sistemas de información.	MEDIO	MEDIO	30	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
PO11	Administración de la calidad	Cumplir con los requerimientos del cliente de TI				
11.13	Estándares para Pruebas de Sistemas	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 la prueba total del sistema, como parte de cada proyecto de desarrollo o modificación de sistemas de información.	MEDIO	MEDIO	30	
11.14	Pruebas Piloto/En Paralelo	La metodología del ciclo de vida de desarrollo de sistemas de la organización debe definir las condiciones bajo las cuales deberán conducirse las pruebas piloto o en paralelo de sistemas nuevos y/o actuales.	BAJO	MEDIO	6	
11.15	Documentación de las Pruebas del Sistema	La metodología del ciclo de vida de desarrollo de sistemas de la organización debe disponer, como parte de cualquier proyecto de desarrollo, implementación o modificación de sistemas de información, que se conserve la documentación de los resultados de las pruebas del sistema.	MEDIO	MEDIO-BAJO	20	
11.16	Evaluación del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares de Desarrollo	El enfoque de aseguramiento de calidad de la organización deberá requerir que una revisión post - implementación de un sistema de información operacional evalúe si el equipo encargado del proyecto, cumplió con las estipulaciones de la metodología del ciclo de vida de desarrollo de sistemas.	MEDIO-ALTO	MEDIO	42	
11.17	Revisión del Aseguramiento de Calidad sobre el Logro de los Objetivos de TI	El enfoque de aseguramiento de calidad deberá incluir una revisión de hasta qué punto los sistemas particulares y las actividades de desarrollo de aplicaciones han alcanzado los objetivos de la función de servicios de información.	MEDIO-ALTO	MEDIO	42	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
PO11	Administración de la calidad	Cumplir con los requerimientos del cliente de TI				
11.18	Métricas de calidad	La gerencia deberá definir y utilizar métricas para medir los resultados de actividades, evaluando si las metas de calidad han sido alcanzadas.	MEDIO-ALTO	MEDIO-BAJO	28	
11.19	Reportes de Revisiones de Aseguramiento de Calidad	Los reportes de revisiones de aseguramiento de calidad deberán ser preparados y enviados a la Gerencia de los departamentos usuarios y de la función de servicios de información (TI).	MEDIO-ALTO	MEDIO-BAJO	28	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
AI6	Administrar cambios	Minimizar la posibilidad de interrupciones, alteraciones no autorizadas, y los errores				
6.1	Inicio y Control de Solicitudes de Cambio	La Gerencia deberá asegurar que todas las solicitudes de cambios tanto internos como por parte de proveedores estén estandarizados y sujetos a procedimientos formales de administración de cambios. Las solicitudes deberán categorizarse y priorizarse y se deben establecer procedimientos específicos para manejar cambios urgentes. Los solicitantes de los cambios deben permanecer informados acerca del estatus de su solicitud.	MEDIO-BAJO	ALTO	30	
6.2	Análisis de Impacto	Deberá establecerse un procedimiento para asegurar que todas las solicitudes de cambio sean evaluadas en una forma estructurada que considere todos los posibles impactos que el cambio pueda ocasionar sobre el sistema operacional y su funcionalidad.	MEDIO-BAJO	MEDIO-ALTO	24	
6.3	Control de Cambios	La Gerencia de TI deberá asegurar que la administración de cambios, así como el control y la distribución de software sean integrados apropiadamente en un sistema completo de administración de configuración. El sistema utilizado para monitorear los cambios a los sistemas de aplicación debe ser automático para soportar el registro y seguimiento de los cambios realizados a grandes y complejos sistemas de información.	MEDIO-ALTO	MEDIO-ALTO	56	
6.4	Cambios de Emergencia	La gerencia de TI debe establecer parámetros definiendo cambios de emergencia y procedimientos para controlar estos cambios cuando ellos traspasan los procesos normales de análisis de prioridades de la gerencia para su implementación. Los cambios de emergencia deben ser registrados y autorizados por la gerencia de TI antes de su implementación.	MEDIO-BAJO	MEDIO-ALTO	24	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
AI6	Administrar cambios	Minimizar la posibilidad de interrupciones, alteraciones no autorizadas, y los errores				
6.5	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.	MEDIO	MEDIO	30	
6.6	Mantenimiento Autorizado	La Gerencia de TI deberá asegurar que el personal de mantenimiento tenga asignaciones específicas y que su trabajo sea monitoreado apropiadamente. Además, sus derechos de acceso al sistema deberán ser controlados para evitar riesgos de accesos no autorizados a los sistemas automatizados.	MEDIO	MEDIO	30	
6.7	Política de Liberación de Software	La Gerencia de TI deberá garantizar que la liberación de software esté regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.	MEDIO	MEDIO	30	
6.8	Distribución de Software	Deberán establecerse medidas de control específicas para asegurar la distribución del elemento de software correcto al lugar correcto, con integridad y de manera oportuna y con adecuadas pistas de auditoría.	MEDIO	MEDIO-ALTO	40	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS4	Asegurar el servicio continuo	Tener la seguridad de que los servicios de TI estén disponibles cuando se requieran y asegurar un impacto mínimo en el negocio en el evento de una interrupción mayor				
4.1	Marco de Referencia de Continuidad de Tecnología de información	La Gerencia de TI, en cooperación con los propietarios de los procesos del negocio, deberá crear un marco de referencia de continuidad que defina los roles, responsabilidades, el enfoque/metodología basada en riesgo a seguir y las reglas y la estructura para documentar el plan de continuidad, así como los procedimientos de aprobación.	MEDIO	MEDIO	30	
4.2	Estrategia y Filosofía del Plan de Continuidad de TI	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.	MEDIO-ALTO	MEDIO-ALTO	56	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS4	Asegurar el servicio continuo	Tener la seguridad de que los servicios de TI estén disponibles cuando se requieran y asegurar un impacto mínimo en el negocio en el evento de una interrupción mayor				
4.3	Contenido del Plan de Continuidad de TI	La Gerencia de TI deberá asegurar que se desarrolle un plan escrito conteniendo lo siguiente: +Guías sobre la utilización del Plan de Continuidad; +Procedimientos de emergencia para asegurar la integridad de todo el personal afectado; +Procedimientos de respuesta definidos para regresar al negocio al estado en que se encontraba antes del incidente o desastre; +Procedimientos para salvaguardar y reconstruir las instalaciones; +Procedimientos de coordinación con las autoridades públicas; +Procedimientos de comunicación con los socios y demás interesados: empleados, clientes clave, proveedores críticos, accionistas y gerencia + Información crítica sobre grupos de continuidad, personal afectado, clientes, proveedores, autoridades públicas y medios de comunicación.	ALTO	ALTO	90	No existe un plan de Continuidad del TI, pero existen ciertos procedimientos no formalizados que podrian ayudar en el caso de darse una contingencia: + Se conoce a las personas que se debe notificar en caso de suceder una emergencia. + Se conoce en donde estan almacenados los respaldos. + Los procesos de respaldo de datos son ejecutados de manera diaria. + Se cuenta con un centro de computo alternativo desde donde se podría continuar con la atención de servicios de IT.
4.4	Reducción de requerimientos de Continuidad de Tecnología de Información.	La Gerencia de servicios de información deberá establecer procedimientos y guías para minimizar los requerimientos de continuidad con respecto a personal, instalaciones, hardware, software, equipo, formatos, consumibles y mobiliario.	MEDIO	MEDIO	30	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS4	Asegurar el servicio continuo	Tener la seguridad de que los servicios de TI estén disponibles cuando se requieran y asegurar un impacto mínimo en el negocio en el evento de una interrupción mayor				
4.5	Mantenimiento del Plan de Continuidad de Tecnología de Información	La Gerencia de TI deberá proveer procedimientos de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja requerimientos de negocio actuales. Esto requiere de procedimientos de mantenimiento del plan de continuidad alineados con el cambio, la administración y los procedimientos de recursos humanos.	ALTO	ALTO	90	No existe un plan de Continuidad del TI, por ende tampoco existen procedimientos de control de cambios.
4.6	Pruebas del Plan de Continuidad de TI	Para contar con un Plan efectivo de Continuidad, la gerencia necesita evaluar su adecuación de manera regular o cuando se presenten cambios mayores en el negocio o en la infraestructura de TI; esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas e implementar un plan de acción de acuerdo con los resultados.	ALTO	ALTO	90	No existe un plan de Continuidad de TI
4.7	Entrenamiento sobre el Plan de Continuidad de Tecnología de Información	La metodología de Continuidad ante desastres deberá asegurar que todas las partes interesadas reciban sesiones de entrenamiento regulares con respecto a los procedimientos a ser seguidos en caso de un incidente o un desastre.	ALTO	MEDIO-ALTO	72	No existe un plan de Continuidad de TI
4.8	Distribución del Plan de Continuidad de TI	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.	ALTO	MEDIO-ALTO	72	No existe un plan de Continuidad de TI

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS4	Asegurar el servicio continuo	Tener la seguridad de que los servicios de TI estén disponibles cuando se requieran y asegurar un impacto mínimo en el negocio en el evento de una interrupción mayor				
4.9	Procedimientos de respaldo de procesamiento alternativo para Departamentos usuarios	La metodología de continuidad deberá asegurar que los departamentos usuarios establezcan procedimientos alternativos de procesamiento, que puedan ser utilizados hasta que la función de servicios de información sea capaz de restaurar completamente sus servicios después de un evento o un desastre.	MEDIO-BAJO	MEDIO-ALTO	24	
4.10	Recursos Críticos de Tecnología de Información	El plan de continuidad deberá identificar los programas de aplicación, servicios de terceros, sistemas operativos, personal, insumos, archivos de datos que resultan críticos así como los tiempos necesarios para la recuperación después de que se presenta un desastre. Los datos y las operaciones críticas deben ser identificadas, documentadas, priorizadas y aprobadas por los dueños de los procesos del negocio en cooperación con la Gerencia de TI.	ALTO	MEDIO-ALTO	72	No existe un plan de Continuidad del TI, pero se tiene conciencia de cuales son los recursos de IT de importancia
4.11	Sitio y Hardware de Respaldo	La Gerencia deberá asegurar que la metodología de continuidad incorpora la identificación de alternativas relativas al sitio y al hardware de respaldo, así como una selección alternativa final. En caso de aplicar, deberá establecerse un contrato formal para este tipo de servicios.	MEDIO	ALTO	50	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS4	Asegurar el servicio continuo	Tener la seguridad de que los servicios de TI estén disponibles cuando se requieran y asegurar un impacto mínimo en el negocio en el evento de una interrupción mayor				
4.12	Almacenamiento de respaldo en el sitio alterno (Off-site)	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 del negocio y el personal de la función de TI deben involucrarse en determinar que recursos de respaldo deben ser almacenados en el sitio alterno. La instalación de almacenamiento externo debe contar con medidas 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 alterno son periódicamente analizados, al menos una vez al año, para garantizar que ofrezca seguridad y protección ambiental.	MEDIO	ALTO	50	
4.13	Procedimiento de afinamiento del Plan de Continuidad	Dada una exitosa reanudación de la función de TI después de un desastre, la gerencia de servicios de información deberá establecer procedimientos para evaluar lo adecuado del plan y actualizarlo de acuerdo con los resultados de dicha evaluación.	ALTO	MEDIO	54	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS5	Garantizar la seguridad de los sistemas	Salvaguardar la información contra el uso no autorizado, divulgación o modificación, daño o pérdida.				
5.1	Administrar Medidas de Seguridad	La seguridad en TI deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. Esto incluye: + Trasladar información sobre evaluación de riesgos a los planes de seguridad de TI; + Implementar el plan de seguridad de TI; + Actualizar el plan de seguridad de TI para reflejar cambios en la configuración de TI; + Evaluar el impacto de las solicitudes de cambio en la seguridad de TI; + Monitorear la implementación del plan deseguridad de TI; y + Alinear los procedimientos de seguridad de TI a otras políticas y procedimientos	ALTO	MEDIO-ALTO	72	No existe un plan de seguridad
5.2	Identificación, Autenticación y Acceso	El acceso lógico y el uso de los recursos de TI deberá restringirse a través de la implementación de mecanismos adecuados de identificación, autenticación y autorización relacionando los usuarios y los recursos con las reglas de acceso. Dicho mecanismo deberá evitar que personal no autorizado, conexiones telefónicas por marcado y otros puertos de entrada al sistema (redes) tengan acceso a los recursos de cómputo, de igual forma deberá minimizar la necesidad de autorizar usuarios para usar múltiples sign-ons. Asimismo deberán establecerse procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso (por ejemplo, cambios periódicos de contraseñas o passwords).	MEDIO-BAJO	MEDIO-ALTO	24	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS5	Garantizar la seguridad de los sistemas	Salvaguardar la información contra el uso no autorizado, divulgación o modificación, daño o pérdida.				
5.3	Seguridad de Acceso a Datos en Línea	En un ambiente de tecnología de información en línea, la Gerencia de TI 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.	MEDIO-BAJO	MEDIO-ALTO	24	
5.4	Administración de Cuentas de Usuario	La Gerencia deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la solicitud, establecimiento, emisión, suspensión y cierre 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. La seguridad de acceso a terceros debe definirse contractualmente teniendo en cuenta requerimientos de administración y no revelación.	MEDIO	MEDIO-ALTO	40	
5.5	Revisión Gerencial de Cuentas de Usuario	La Gerencia deberá contar con un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso. Se debe llevar a cabo la comparación periódica entre los recursos y los registros de las cuentas para reducir el riesgo de errores, fraudes, alteración no autorizada o accidental.	MEDIO-ALTO	MEDIO	42	
5.6	Control de Usuarios sobre Cuentas de Usuario	Los usuarios deberán controlar en forma sistemática la actividad de su(s) propia(s) cuenta (s). También se deberán establecer mecanismos de información para permitirles supervisar la actividad normal, así como alertarlos oportunamente sobre actividades inusuales.	MEDIO-ALTO	MEDIO-ALTO	56	

OBJETIVOS DE CONTROL	OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN

DS5	Garantizar la seguridad de los sistemas	Salvaguardar la información contra el uso no autorizado, divulgación o modificación, daño o pérdida.				
5.7	Vigilancia de Seguridad	La administración de seguridad de TI debe asegurar que la actividad de seguridad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente a todos aquellos que puedan verse afectados, tanto interna como externamente y se debe actuar de una manera oportuna.	MEDIO-ALTO	MEDIO-ALTO	56	
5.8	Clasificación de Datos	La Gerencia deberá implementar procedimientos para asegurar que todos los datos son clasificados en términos de sensitividad, mediante una decisión explícita y formal del dueño de los datos de acuerdo con el esquema de clasificación de datos. Aún los datos que “no requieren protección” deberán contar con una decisión formal que les asigne dicha clasificación. Los dueños deben determinar la ubicación o disposición de sus datos y determinar quienes pueden compartir los datos aun si y cuando los programas y archivos sean mantenidos, archivados o borrados. Debe quedar evidencia de la aprobación del dueño y de la disposición del dato. Se deben definir políticas para soportar la reclasificación de la información, basados sobre cambios en la sensitividad. El esquema de clasificación debe incluir criterios para administrar el intercambio de información entre organizaciones, teniendo en cuenta tanto la seguridad y el cumplimiento como la legislación relevante.	MEDIO-ALTO	MEDIO	42	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS5	Garantizar la seguridad de los sistemas	Salvaguardar la información contra el uso no autorizado, divulgación o modificación, daño o pérdida.				
5.9	Administración de Derechos de Acceso e Identificación Centralizada	Deben existir controles para asegurar que la identificación y los derechos de acceso de los usuarios, así como la identidad del sistema y la propiedad de los datos, son establecidos y administrados de forma única y centralizada, para obtener consistencia y eficiencia de un control de acceso global.	MEDIO-BAJO	MEDIO-ALTO	24	
5.10	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 logs) deberá otorgarse tomando como base el principio de menor privilegio o necesidad de saber.	MEDIO-ALTO	MEDIO-ALTO	56	
5.11	Manejo de Incidentes	La Gerencia deberá implementar la capacidad de manejar incidentes de seguridad computacional, dar atención a dichos incidentes mediante el establecimiento de una plataforma centralizada con suficiente experiencia y equipada con instalaciones de comunicación rápidas y seguras. Deberán establecerse las responsabilidades y los procedimientos de manejo de incidentes para asegurar una respuesta apropiada, efectiva y oportuna a los incidentes de seguridad.	MEDIO	MEDIO-ALTO	40	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS5	Garantizar la seguridad de los sistemas	Salvaguardar la información contra el uso no autorizado, divulgación o modificación, daño o pérdida.				
5.12	Reacreditación	La Gerencia deberá asegurar que se lleve a cabo periódicamente una reacreditación de seguridad (por ejemplo, a través de equipos de personal técnico “tigre”) con el fin de mantener actualizado el nivel de seguridad aprobado formalmente y la aceptación del riesgo residual.	ALTO	MEDIO-BAJO	36	
5.13	Confianza en Contrapartes	Las políticas organizacionales deberán asegurar que se implementen prácticas de control para verificar la autenticidad de las contrapartes que proporcionan instrucciones o transacciones electrónicas. Esto puede lograrse mediante el intercambio confiable de passwords, tokens o llaves criptográficas.	MEDIO-ALTO	BAJO	14	
5.14	Autorización de transacciones	Las políticas organizacionales deberán asegurar que, en donde sea apropiado, se implementen controles para proporcionar autenticidad a las transacciones y establecer la validez de la identificación solicitada por el usuario ante el sistema. Esto requiere el empleo de técnicas criptográficas para “firmar” y verificar transacciones.	MEDIO-BAJO	BAJO	6	
5.15	No negación o no rechazo	Las políticas organizacionales deberán asegurar que, en donde sea apropiado, las transacciones no puedan ser negadas por ninguna de las partes participantes en la operación y que se implementen controles para que no se pueda negar el origen o destino de la transacción y que se pueda probar que se envió y recibió la transacción. Esto puede lograrse a través de firmas digitales, registro de tiempos y terceros confiables, y adicionalmente con políticas apropiadas que tengan en cuenta los requerimientos regulatorios relevantes.	MEDIO	BAJO	10	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS5	Garantizar la seguridad de los sistemas	Salvaguardar la información contra el uso no autorizado, divulgación o modificación, daño o pérdida.				
5.16	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 (trusted paths). La información sensitiva incluye: información sobre administración de seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas. Para lograr esto, se pueden establecer canales confiables utilizando encripción entre usuarios, entre usuarios y sistemas y entre sistemas.	MEDIO	BAJO	10	
5.17	Protección de las funciones de seguridad	Todo el hardware y software relacionado con seguridad debe encontrarse permanentemente protegido contra intromisiones para proteger su integridad y contra divulgación de sus claves secretas. Adicionalmente, la organización deberá mantener discreción sobre el diseño de su seguridad, pero no basar la seguridad en mantener el diseño como secreto.	BAJO	MEDIO-ALTO	8	
5.18	Administración de Llaves Criptográficas	La Gerencia deberá definir e implementar procedimientos y protocolos a ser utilizados en la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas contra modificaciones y divulgación no autorizada. Si una llave se encuentra comprometida (en riesgo), la gerencia deberá asegurarse de que esta información se hace llegar a todas las partes interesadas a través de una lista de revocación de certificados o mecanismos similares.	ALTO	BAJO	18	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS5	Garantizar la seguridad de los sistemas	Salvaguardar la información contra el uso no autorizado, divulgación o modificación, daño o pérdida.				
5.19	Prevención, Detección y Corrección de Software "Malicioso"	Con respecto al software malicioso, tal como los virus computacionales o Caballos de Troya, la Gerencia deberá establecer un marco de referencia de adecuadas medidas de control preventivas, detectivas y correctivas y responder y reportar su presencia. Las Gerencias de TI y de negocios deben asegurar que se establezcan procedimientos a través de toda la organización para proteger los sistemas de información contra virus computacionales. Los procedimientos deben incorporar protección contra virus, detección, respuesta ante su presencia y reporte.	BAJO	MEDIO-ALTO	8	
5.20	Arquitectura de Firewalls y conexión a redes públicas	La organización deberá contar con Firewall adecuados para proteger contra negación de servicios y cualquier acceso no autorizado a los recursos internos si existe conexión con Internet u otras redes públicas; se deberá controlar en ambos sentidos cualquier aplicación y el flujo de administración de infraestructura y se deberá proteger contra ataques de negación del servicio.	MEDIO-BAJO	MEDIO-ALTO	24	
5.21	Protección de Valores Electrónicos	La Gerencia debe proteger la integridad continuada de todas las tarjetas o mecanismos de seguridad física similares, utilizadas para autenticación o almacenamiento de información financiera o sensitiva tomando en consideración las instalaciones o equipos relacionados, los dispositivos, los empleados y los métodos de validación utilizados.	MEDIO	MEDIO-BAJO	20	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS11	Administración de datos	Asegurar que los datos permanezcan completos, precisos y válidos durante su captura, procesamiento y almacenamiento				
11.1	Procedimientos de Preparación de Datos	La Gerencia deberá establecer procedimientos de preparación de datos que deben 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.	MEDIO-BAJO	MEDIO	18	
11.2	Procedimientos de Autorización de Documentos Fuente	La Gerencia deberá asegurar que los documentos fuente sean preparados apropiadamente por personal autorizado que actúa dentro de su autoridad, y que se establezca una separación de funciones adecuada con respecto al origen y aprobación de documentos fuente.	MEDIO-BAJO	MEDIO-ALTO	24	
11.3	Recopilación de Datos de Documentos Fuente	Los procedimientos de la organización deberán asegurar que todos los documentos fuente autorizados estén completos, sean precisos, registrados apropiadamente y transmitidos oportunamente para su ingreso a proceso.	MEDIO-BAJO	MEDIO-ALTO	24	
11.4	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.	MEDIO	MEDIO	30	
11.5	Retención de Documentos Fuente	Deberán establecerse procedimientos para asegurar que la organización pueda retener o reproducir los documentos fuente originales durante un período de tiempo razonable para facilitar la recuperación o reconstrucción de datos, así como para satisfacer requerimientos legales.	MEDIO-BAJO	MEDIO-ALTO	24	

OBJETIVOS DE CONTROL	OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN

DS11	Administración de datos	Asegurar que los datos permanezcan completos, precisos y válidos durante su captura, procesamiento y almacenamiento				
11.6	Procedimientos de Autorización de Entrada de Datos	La organización deberá establecer procedimientos apropiados para asegurar que la entrada de datos sea llevada a cabo únicamente por personal autorizado.	MEDIO-BAJO	MEDIO	18	
11.7	Chequeos de Exactitud, Suficiencia y Autorización	Los datos de transacciones, ingresados 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.	MEDIO-ALTO	MEDIO-ALTO	56	
11.8	Manejo de Errores en la Entrada de Datos	La organización deberá establecer procedimientos para la corrección y reenvío de datos que hayan sido capturados erróneamente.	MEDIO	MEDIO	30	
11.9	Integridad de Procesamiento de Datos	La organización deberá establecer procedimientos para el procesamiento de datos que aseguren que la segregación de funciones sea mantenida y que el trabajo realizado sea verificado rutinariamente. Los procedimientos deberán asegurar que se establezcan controles de actualización adecuados como totales de control "corrida a corrida –run to run-" y controles de actualización de archivos maestros.	MEDIO	MEDIO-ALTO	40	
11.10	Validación y Edición de Procesamiento de Datos	La organización deberá establecer procedimientos para asegurar que la validación, autenticación y edición del procesamiento sean llevadas a cabo tan cerca del punto de origen como sea posible.	MEDIO-BAJO	MEDIO-BAJO	12	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS11	Administración de datos	Asegurar que los datos permanezcan completos, precisos y válidos durante su captura, procesamiento y almacenamiento				
11.11	Manejo de Errores en el Procesamiento de Datos	La organización deberá establecer procedimientos para el 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.	MEDIO-BAJO	MEDIO	18	
11.12	Manejo y Retención de Datos de Salida	La organización deberá establecer procedimientos para el manejo y la retención de datos producidos por sus programas de aplicación de TI. En caso de que instrumentos negociables (ej. Títulos valores) sean los receptores de la salida, se deberá prestar especial cuidado en prevenir usos inadecuados.	MEDIO-BAJO	MEDIO-ALTO	24	
11.13	Distribución de Datos Salidos de los Procesos	La organización deberá establecer y comunicar procedimientos escritos para la distribución de datos de salida de tecnología de información.	MEDIO	MEDIO-BAJO	20	
11.14	Balanceo y Conciliación de Datos de Salida	La organización deberá establecer procedimientos para asegurar que los datos de salida sean balanceados rutinariamente con los totales de control relevantes. Deberán existir pistas de auditoría para facilitar el seguimiento del procesamiento de transacciones y la conciliación de datos con problema.	MEDIO	MEDIO	30	
11.15	Revisión de Datos de Salida y Manejo de Errores	La Gerencia de la organización deberá establecer procedimientos para asegurar que la precisión de los reportes de los datos de salida sea revisada por el proveedor y por los usuarios responsables. Asimismo, deberán establecerse procedimientos para controlar los errores contenidos en los datos de salida.	MEDIO-BAJO	MEDIO	18	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS11	Administración de datos	Asegurar que los datos permanezcan completos, precisos y válidos durante su captura, procesamiento y almacenamiento				
11.16	Provisiones de Seguridad para Reportes de Salida	La organización deberá establecer procedimientos para garantizar que la seguridad de los reportes generados por los procesos sea mantenida para todos aquellos reportes que estén por distribuirse, así como para todos aquéllos que ya hayan sido distribuidos a los usuarios.	MEDIO-ALTO	MEDIO-ALTO	56	
11.17	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.	MEDIO-ALTO	MEDIO-ALTO	56	
11.18	Protección de Información Sensitiva Desechada	La Gerencia deberá definir e implementar procedimientos para impedir el acceso a la información sensitiva, al software de las computadoras, a los discos y otros equipos o medios cuando los mismos son desechados o transferidos a otro uso. Tales procedimientos deberán garantizar que ninguna información marcada como “borrada” o “desechada”, pueda ser accedida por personas internas o externas a la organización.	MEDIO-ALTO	MEDIO	42	
11.19	Administración de Almacenamiento	Deberán desarrollarse procedimientos para el almacenamiento de datos que consideren requerimientos de recuperación, de economía y así mismo tengan en cuenta las políticas de seguridad de la organización.	MEDIO-BAJO	MEDIO-ALTO	24	
11.20	Períodos de Retención y Términos de Almacenamiento	Deberán definirse los períodos de retención y los términos de almacenamiento para documentos, datos, programas, reportes y mensajes (de entrada y de salida), así como los datos (claves, certificados) utilizados para su encripción y autenticación.	MEDIO-BAJO	MEDIO-ALTO	24	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS11	Administración de datos	Asegurar que los datos permanezcan completos, precisos y válidos durante su captura, procesamiento y almacenamiento				
11.21	Sistema de Administración de la Librería de Medios	La función de servicios de información deberá establecer procedimientos para asegurar que el contenido de su librería de medios sea inventariado sistemáticamente, que cualquier discrepancia revelada por un inventario físico sea solucionada oportunamente y que se consideren las medidas necesarias para mantener la integridad de los medios magnéticos almacenados en la librería.	MEDIO-ALTO	MEDIO-ALTO	56	
11.22	Responsabilidades de la Administración de la Librería de Medios	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 soporte y registro. Las responsabilidades sobre el manejo de la librerías de medios (cintas magnéticas, cartuchos, discos y disquetes) deberán ser asignadas a miembros específicos del personal de servicios de información.	MEDIO-BAJO	MEDIO-ALTO	24	
11.23	Respaldo (Back-up) y Restauración	La Gerencia deberá implementar una estrategia apropiada de respaldo y recuperación 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.	MEDIO-BAJO	ALTO	30	
11.24	Funciones de Respaldo	Deberán establecerse procedimientos para asegurar que los respaldos sean realizados de acuerdo con la estrategia de respaldo definida, y que las copias de respaldo sean verificadas regularmente.	MEDIO-BAJO	MEDIO-ALTO	24	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS11	Administración de datos	Asegurar que los datos permanezcan completos, precisos y válidos durante su captura, procesamiento y almacenamiento				
11.25	Almacenamiento de Respaldos	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 archivos de datos y otros elementos.	MEDIO-BAJO	MEDIO-ALTO	24	
11.26	Archivo	La Gerencia deberá implementar una política y procedimientos para asegurar que el archivo cumple con requerimientos legales y de negocio y que se encuentra debidamente protegido y su información adecuadamente registrada.	MEDIO-ALTO	MEDIO	42	
11.27	Protección de Mensajes Sensitivos	Con respecto a la transmisión de datos a través de Internet u otra red pública, la Gerencia deberá definir e implementar procedimientos y protocolos que deben ser utilizados para el aseguramiento de la integridad, confidencialidad y “no negación/rechazo” de mensajes sensitivos.	MEDIO-ALTO	BAJO	14	
11.28	Autenticación e Integridad	Antes que alguna acción crítica sea tomada sobre información originada fuera de la Organización, que se reciba vía teléfono, correo de voz, documentos (en papel), fax o correo electrónico, se deberá verificar adecuadamente la autenticidad e integridad de dicha información.	MEDIO-ALTO	BAJO	14	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS11	Administración de datos	Asegurar que los datos permanezcan completos, precisos y válidos durante su captura, procesamiento y almacenamiento				
11.29	Integridad de Transacciones Electrónicas	Tomando en consideración que las fronteras tradicionales de tiempo y de geografía son menos precisas y confiables, la Gerencia deberá definir e implementar apropiados procedimientos y prácticas para transacciones electrónicas que sean sensitivas y críticas para la Organización, que permitan asegurar su integridad y autenticidad de: + atomicidad (unidad de trabajo indivisible, todas sus acciones tienen éxito o todas ellas fallan) + consistencia (si la transacción no logra alcanzar un estado final estable, deberá regresar al sistema a su estado inicial); + aislamiento (el comportamiento de una transacción no es afectado por otras transacciones que se ejecutan concurrentemente); y + durabilidad (los efectos de una transacción son permanentes después que concluye su proceso, los cambios que origina deben sobrevivir a fallas de sistema)	ALTO	BAJO	18	
11.30	Integridad Continua de Datos Almacenados	La Gerencia deberá asegurar que la integridad y lo adecuado de los datos mantenidos en archivos y otros medios (ej. tarjetas electrónicas) se verifique periódicamente. Atención específica deberá darse a dispositivos de tokens, archivos de referencia y archivos que contengan información privada.	MEDIO-BAJO	BAJO	6	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS12	Administración de instalaciones	Proveer un entorno físico adaptable el cual proteja al equipo y personas de TI contra los peligros naturales y provocados por el hombre.				
12.1	Seguridad Física	Deberán establecerse medidas apropiadas de seguridad física y medidas de control de acceso para las instalaciones de tecnología de información incluyendo el uso de dispositivos de información off-site en conformidad con la política general de seguridad. La seguridad física y los controles de acceso deben abarcar no sólo el área que contenga el hardware del sistema sino también las ubicaciones del cableado usado para conectar elementos del sistema, servicios de soporte (como la energía eléctrica), medios de respaldo y demás elementos requeridos para la operación del sistema. El acceso deberá restringirse a las personas que hayan sido autorizadas. Cuando los recursos de tecnología de información estén ubicados en áreas públicas, deberán estar debidamente protegidos para impedir o para prevenir pérdidas o daños por robo o por vandalismo.	MEDIO-ALTO	ALTO	70	No existe una política o procedimientos de seguridad formalmente definidos. Pero el acceso a los servidores y al área de cableado estructurado esta restringido.
12.2	Discreción sobre las Instalaciones de Tecnología de Información	La Gerencia de la función de servicios de información deberá asegurar que se mantenga un bajo perfil sobre la identificación física de las instalaciones relacionadas con sus operaciones de tecnología de información. La información sobre la ubicación del sitio debe ser limitada y mantenerse con la adecuada reserva.	MEDIO-ALTO	MEDIO	42	
12.3	Escolta de Visitantes	Deberán establecerse procedimientos apropiados que aseguren que las personas que no formen parte del grupo de operaciones de la función de servicios de información sean escoltadas por algún miembro de ese grupo cuando deban entrar a las instalaciones de cómputo. Deberá mantenerse y revisarse regularmente una bitácora de visitantes.	ALTO	MEDIO	54	

OBJETIVOS DE CONTROL			OCURRENCIA	IMPACTO	RIESGO	JUSTIFICACIÓN
DS12	Administración de instalaciones	Proveer un entorno físico adaptable el cual proteja al equipo y personas de TI contra los peligros naturales y provocados por el hombre.				
12.4	Salud y Seguridad del Personal	Deberán establecerse y mantenerse prácticas de salud y seguridad en línea con las leyes y regulaciones internacionales, nacionales, regionales, estatales y locales.	MEDIO-ALTO	MEDIO-BAJO	28	
12.5	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.	MEDIO-ALTO	MEDIO	42	
12.6	Suministro Ininterrumpido de Energía	La Gerencia deberá evaluar regularmente la necesidad de contar con generadores y baterías de suministro ininterrumpido de energía (UPS) para las aplicaciones críticas de tecnología de información, con el fin de protegerse contra fallas y fluctuaciones de energía. Cuando sea justificable, deberá instalarse el equipo más apropiado.	BAJO	MEDIO-ALTO	8	

7.2.4 Evaluar y Priorizar Riesgos

Las comparaciones del análisis de riesgo realizadas sobre diferentes áreas de la organización o sobre los diferentes procesos permiten priorizar los riesgos sobre los cuales se ha de centrar la atención para definir una opción de tratamiento.

Se ha elaborado una lista ordenada de mayor a menor, por la valoración del nivel de exposición. Esto permite definir los riesgos de mayor grado de importancia sobre los cuales deberá definir las opciones de tratamiento. Centrando nuestra atención en lo crítico, de acuerdo a los niveles de aceptación que se han definidos

A continuación se detalla un resumen del nivel de exposición de los riesgos.

Procesos	**Objetivos de Control**	**Alto**	**Medio**	**Bajo**	**Alto+Medio**
DS4 - Asegurar continuidad del servicio	13	6	4	3	10
DS5 - Garantizar la seguridad de sistemas	21	1	8	12	9
DS11 - Administrar la información	30	0	7	23	7
PO9 - Evaluar Riesgos	8	0	6	2	6
PO11 -Administrar Calidad	19	0	6	13	6
DS12 - Administrar las instalaciones	6	1	3	2	4
AI6 - Administrar cambios	8	0	2	6	2
	105	8	36	61	44
		8%	34%	58%	42%

Los **riesgos a priorizar** son los que están en el nivel de exposición ALTO y MEDIO.

7.2.5 Tratamiento del Riesgo

Para la actividad o componente al cual se aplicó el proceso de administración de riesgos, hay que determinar las posibles formas de reducir o mitigar el riesgo.

Entre las opciones de tratamiento tenemos las siguientes:

Evitar: Se reduce la probabilidad de pérdida al mínimo; dejar de ejercer la actividad o proceso.

Reducir: Se consigue mediante la optimización de los procedimientos y la implementación de controles tendientes a disminuir la probabilidad de ocurrencia o el impacto.

Atomizar: Distribuir la localización del riesgo, segmentando el objeto sobre el cual se puede materializar el riesgo.

Transferir: Pasar el riesgo de un lugar a otro, compartir con otro el riesgo, esta técnica no reduce la probabilidad ni el impacto, involucra a otro en la responsabilidad.

Asumir: Se acepta la pérdida residual probable, con la aceptación del riesgo las estrategias de prevención se vuelven esenciales.

El tratamiento a usar para mitigar los riesgos de alto impacto es estableciendo controles que ayuden a reducir el impacto y probabilidad de ocurrencia de eventos que puedan ocasionar daños a la infraestructura de IT.

Los controles a implementar están enfocados a los siguientes procesos de Administración de IT.

DOMINIO	PROCESO	
Planeación y Organización	PO9	Evaluar riesgos
	PO11	Administrar Calidad
Adquisición e Instalación	AI6	Administrar cambios
Entrega de Servicios	DS4	Asegurar continuidad del servicio
	DS5	Garantizar la seguridad de sistemas
	DS11	Administrar la información
	DS12	Administrar las instalaciones

8. PLAN DE ACCIÓN

<table>
<tr><th colspan="4">MODELO DE MEJORES PRACTICAS – COBIT</th></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 1/3</td></tr>
<tr><td colspan="4">PLAN DE ACCIÓN</td></tr>
<tr><td>DOMINIO :</td><td>PLANIFICACIÓN Y ORGANIZACIÓN</td><td>PROCESO:</td><td>PO9 – Evaluar Riesgo</td></tr>
<tr><td>que satisface los requerimientos de negocio de:</td><td colspan="3">Soportar las decisiones de la administración a través del el logro de los objetivos de TI y responder a las amenazas reduciendo su complejidad incrementando su objetividad e identificando factores de decisión importantes</td></tr>
<tr><td>se hace posible a través de:</td><td colspan="3">la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, involucrando funciones multidisciplinarias y tomando medidas económicas para mitigar los riesgos.</td></tr>
<tr><td>y toma en consideración:</td><td colspan="3">• Propiedad y registro de la administración del riesgo
• diferentes tipos de riesgos de TI (por ejemplo: tecnológicos, de seguridad, de continuidad, regulatorios, etc.)
• Definir y comunicar el perfil de tolerancia del riesgo
• Análisis del origen de las causas y sesiones de tormentas de ideas sobre riesgos
• Medición cuantitativa y/o cualitativa del riesgo
• metodología de evaluación de riesgos
• plan de acción de riesgos
• Reevaluaciones oportunas</td></tr>
<tr><td colspan="4">CONTROLES</td></tr>
<tr><td>Control a Implementar PO9 – C1</td><td colspan="3">POLÍTICAS Y PROCEDIMIENTOS DE EVALUACIÓN DE RIESGOS.</td></tr>
<tr><td></td><td colspan="3">La administración deberá establecer un foro Gerencial, para asegurarse que exista una dirección clara de las iniciativas de seguridad
• Metodología
• Frecuencia de evaluación
• Evaluaciones de riesgo a nivel global y de sistemas
• Equipo multidiscplinario
• Mantener actualizadas las evaluaciones de riesgo, resultados de auditorías, inspecciones e incidentes
• Políticas de seguros que cubren el riesgo residual.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente General</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">9 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar PO9 – C2</td><td colspan="3">REVISIONES DE GRUPOS ESPECIALIZADOS</td></tr>
<tr><td></td><td colspan="3">La Gerencia debe solicitar la revisión independiente de grupos especializados de seguridad y de tecnología de Información
• Especialista de Seguridad identifican amenazas
• Especialistas de TI identifican los controles</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente General y Gerencia de Sistemas</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">3 meses</td></tr>
</table>

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS – COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 2/3</td></tr>
<tr><td colspan="4">PLAN DE ACCIÓN</td></tr>
<tr><td>DOMINIO :</td><td>PLANIFICACIÓN Y ORGANIZACIÓN</td><td>PROCESO:</td><td>PO9 – Evaluar Riesgo</td></tr>
<tr><td colspan="4">CONTROLES</td></tr>
<tr><td>Control a Implementar PO9 – C3</td><td colspan="3">DEFINICIÓN DE UN MARCO REFERENCIAL DE RIESGOS</td></tr>
<tr><td></td><td colspan="3">La Gerencia deberá establecer una evaluación sistemática de riesgos incorporando:
• Los riesgos de información relevantes para el logro de los objetivos de la organización
• Base de datos para determinar la forma en la que los riesgos deben ser manejados a un nivel aceptable.
• El alcance y los límites de la evaluación de riesgos</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente General</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">2 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar PO9 – C4</td><td colspan="3">PROCEDIMIENTOS DE EVALUACIÓN DE RIESGOS</td></tr>
<tr><td></td><td colspan="3">La gerencia deberá:
• Determinar que los riesgos identificados incluyen factores tanto externos como internos
• Asesores expertos en riesgos deben asegurar las evaluaciones de riesgo
• Revisar los informes de resultados de las auditorías,
• Revisiones de Inspecciones e incidentes identificados.
• Definir un enfoque cuantitativo y/o cualitativo formal para la identificación y medición de riesgos, amenazas y exposiciones.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente General</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">3 meses</td></tr>
<tr><td colspan="4"></td></tr>
</table>

<table>
<tr><td colspan="6">MODELO DE MEJORES PRACTICAS – COBIT</td></tr>
<tr><td colspan="3">EMPRESA : Ecuacolor</td><td colspan="3">Fecha de diagnostico :</td></tr>
<tr><td colspan="5">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 3/3</td></tr>
<tr><td colspan="6">PLAN DE ACCIÓN</td></tr>
<tr><td>DOMINIO :</td><td>PLANIFICACIÓN Y ORGANIZACIÓN</td><td colspan="2">PROCESO:</td><td colspan="2">PO9 – Evaluar Riesgo</td></tr>
<tr><td>Control a Implementar PO9 – C5</td><td colspan="5">REPORTES A LA PRESIDENCIA PARA SU REVISIÓN Y ACUERDO DE ACEPTACIÓN</td></tr>
<tr><td></td><td colspan="5">La Gerencia de Sistemas deberá emitir reportes a la Presidencia para su revisión y acuerdo con los riesgos identificados.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="5">Gerencia de Sistemas</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="5">1 mes</td></tr>
<tr><td>Control a Implementar PO9 – C6</td><td colspan="5">PLAN DE ACCIÓN</td></tr>
<tr><td></td><td colspan="5">La Gerencia deberá establecer el plan de acción contra los riesgos, se debe establecer la estrategia de riesgos en términos de evitar, mitigar o aceptar el riesgo.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="5">Gerente General</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="5">3 meses</td></tr>
</table>

<table>
<tr><td colspan="8">RIESGOS A MITIGAR</td></tr>
<tr><td rowspan="2">Objetivos de Control</td><td colspan="3">Riesgo Actual</td><td colspan="3">Riesgo Esperado</td><td rowspan="2">OBSERVACIÓN</td></tr>
<tr><td>O</td><td>I</td><td>T</td><td>O</td><td>I</td><td>T</td></tr>
<tr><td>Evaluación de Riesgos del Negocio</td><td>7</td><td>8</td><td>56</td><td>3</td><td>8</td><td>24</td><td>PO9-C1, C3, C4</td></tr>
<tr><td>Enfoque de Evaluación de Riesgos</td><td>7</td><td>9</td><td>56</td><td>3</td><td>9</td><td>27</td><td>PO9-C1, C3, C4</td></tr>
<tr><td>Medición de Riesgos</td><td>7</td><td>6</td><td>42</td><td>5</td><td>6</td><td>30</td><td>PO9-C3, C4</td></tr>
<tr><td>Plan de Acción contra Riesgos</td><td>7</td><td>8</td><td>56</td><td>3</td><td>8</td><td>24</td><td>PO9-C3, C6</td></tr>
<tr><td>Aceptación de Riesgos</td><td>7</td><td>6</td><td>42</td><td>5</td><td>6</td><td>30</td><td>PO9-C5, C6</td></tr>
<tr><td>Selección de Garantías o Protecciones</td><td>7</td><td>6</td><td>42</td><td>5</td><td>6</td><td>30</td><td>PO9-C1, C6</td></tr>
</table>

MODELO DE MEJORES PRACTICAS - COBIT			
EMPRESA : Ecuacolor		**Fecha de diagnostico :**	
Diseño de un Sistema de Gestión de Seguridad			Pag 1/2
PLAN DE ACCIÓN			
DOMINIO :	PLANEACIÓN Y ORGANIZACIÓN	**PROCESO:**	PO11 – Administración De la Calidad
que satisface los requerimientos de negocio de:	Satisfacer los requerimientos del cliente de TI		
se hace posible a través de:	La planeación, implementación y mantenimiento de estándares y sistemas de administración provistos para las distintas fases de desarrollo, con entregables claros y responsabilidades explícitas		
y toma en consideración:	Establecimiento de una cultura de calidad • Planes de calidad • responsabilidades de aseguramiento de la calidad • Prácticas de control de calidad • metodología del ciclo de vida de desarrollo de sistemas • Pruebas y documentación de programas y sistemas • revisiones y reporte de aseguramiento de calidad • Entrenamiento e involucramiento del usuario final y del personal de aseguramiento de calidad • Desarrollo de una base de conocimientos de aseguramiento de calidad • Benchmarking contra normas de la industria		
CONTROLES			
Control a Implementar PO11 – C1	**POLÍTICAS Y PROCEDIMIENTOS RELACIONADOS CON EL ASEGURAMIENTO DE LA CALIDAD**		
	La organización deberá desarrollar, diseminar, y periódicamente revisar/actualizar: (i) Una política de administración del Plan General de la Calidad formalmente definida y documentada. (ii) Procedimientos documentados para facilitar la implantación de la política del plan general de calidad y los controles asociados.		
Responsables de implementación	Gerente de Sistemas, Oficial de Seguridad.		
Plazo (tiempo de ejecución)	1 mes		
Control a Implementar PO11 – C2	**METODOLOGÍA DEL CICLO DE VIDA DE DESARROLLO DE SISTEMAS**		
	La organización deberá fijar, realizar, y documentar la metodología adecuada del ciclo de vida en el desarrollo de los sistemas tanto adquirido como desarrollado internamente		
Responsables de implementación	Gerente de Sistemas, Oficial de Seguridad.		
Plazo (tiempo de ejecución)	2 meses		
Control a Implementar PO11 – C3	**MARCO REFERENCIAL DE ADQUISICIÓN Y MANTENIMIENTO PARA LA INFRAESTRUCTURA DE TECNOLOGÍA**		
	La organización deberá construir un marco referencial que incluya pasos a seguir como: adquisición, programación, documentación y pruebas , establecimiento de parámetros y aplicación de correcciones , estos pasos deben estar alineados dentro del marco referencial.		
Responsables de implementación	Gerente de Sistemas, Oficial de Seguridad.		
Plazo (tiempo de ejecución)	2 semanas		
MODELO DE MEJORES PRACTICAS - COBIT			

EMPRESA : Ecuacolor		**Fecha de diagnostico :**	
Diseño de un Sistema de Gestión de Seguridad			Pag 2/2
PLAN DE ACCIÓN			
DOMINIO :	PLANEACIÓN Y ORGANIZACIÓN	**PROCESO:**	PO11 – Administración De la Calidad
Control a Implementar PO11 – C4	**ENFOQUE DE ASEGURAMIENTO DE LA CALIDAD DE LA ORGANIZACIÓN**		
	La organización deberá desarrollar, diseminar, y periódicamente revisar/actualizar: a. Una revisión post-implementación para asegurar que todos los sistemas nuevos ó modificados sean desarrollados y puestos en producción de acuerdo con la metodología del ciclo de vida, el cual debe ser respetado por el equipo del proyecto. b. Una revisión en la medida que los sistemas nuevos ó modificados han alcanzado los objetivos establecidos por la administración.		
Responsables de implementación	Gerente de Sistemas, Oficial de Seguridad.		
Plazo (tiempo de ejecución)	1 mes		

RIESGOS A MITIGAR							
Objetivos de Control	**Riesgo Actual**			**Riesgo Esperado**			**OBSERVACIÓN**
	O	**I**	**T**	**O**	**I**	**T**	
Plan General de Calidad	7	6	**42**	5	6	**30**	PO11-C1-C4
Enfoque de Aseguramiento de Calidad	7	6	**42**	5	6	**30**	PO11-C1-C4
Planeación del Aseguramiento de Calidad	7	6	**42**	5	6	**30**	PO11-C1-C4
Marco de Referencia de Adquisición y Mantenimiento para la Infraestructura de Tecnología	5	10	**50**	3	10	**30**	PO11-C3
Evaluación del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares de Desarrollo	7	6	**42**	5	6	**30**	PO11-C2
Revisión del Aseguramiento de Calidad sobre el Logro de los Objetivos de TI	7	6	**42**	5	6	**30**	PO11-C4

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 1/3</td></tr>
<tr><td colspan="4">PLAN DE ACCIÓN</td></tr>
<tr><td>DOMINIO :</td><td>ADQUISICIÓN E IMPLEMENTACIÓN</td><td>PROCESO:</td><td>AI6-Administrar Cambios</td></tr>
<tr><td>que satisface los requerimientos de negocio de:</td><td colspan="3">Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores</td></tr>
<tr><td>se hace posible a través de:</td><td colspan="3">Un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual.</td></tr>
<tr><td>y toma en consideración:</td><td colspan="3">• identificación de cambios
• procedimientos de categorización, priorización y emergencia
• evaluación del impacto
• autorización de cambios
• Administración de liberación
• distribución de software
• Uso de herramientas automatizadas
• Administración de la configuración
• Rediseño de los procesos del negocio</td></tr>
<tr><td colspan="4">CONTROLES</td></tr>
<tr><td>Control a Implementar AI6 – C1</td><td colspan="3">CONTROL DE CAMBIOS</td></tr>
<tr><td></td><td colspan="3">La Gerencia de TI deberá asegurar que la administración de cambios, así como el control y la distribución de software sean integrados apropiadamente en un sistema completo de administración de configuración. El sistema utilizado para monitorear los cambios a los sistemas de aplicación debe ser automático para soportar el registro y seguimiento de los cambios realizados a grandes y complejos sistemas de información.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerencia de Sistemas</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">8 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar AI6 – C2</td><td colspan="3">SOFTWARE INSTALADO POR EL USUARIO
(USER INSTALLED SOFTWARE)</td></tr>
<tr><td></td><td colspan="3">La organización deberá dar restricciones explícitas para descargar e instalar software por parte de los usuarios</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerencia de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">1 mes</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar AI6 – C3</td><td colspan="3">RESTRICCIONES DE USO DE SOFTWARE.
(SOFTWARE USAGE RESTRICTIONS)</td></tr>
<tr><td></td><td colspan="3">La organización deberá obedecer a las restricciones de uso del software.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerencia de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">4 meses</td></tr>
<tr><td colspan="4"></td></tr>
</table>

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 2/3</td></tr>
<tr><td colspan="4">PLAN DE ACCIÓN</td></tr>
<tr><td>DOMINIO :</td><td>ADQUISICIÓN E IMPLEMENTACIÓN</td><td>PROCESO:</td><td>AI6-Administrar Cambios</td></tr>
<tr><td>Control a Implementar AI6 – C4</td><td colspan="3">DOCUMENTACIÓN DE LOS SISTEMAS DE INFORMACIÓN</td></tr>
<tr><td></td><td colspan="3">La organización deberá asegurar que este disponible la adecuada documentación para el sistema de información y sus componentes constitutivos, protegida cuando es requerido, y distribuida al personal autorizado.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerencia de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">1 mes</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar AI6 – C5</td><td colspan="3">POLÍTICAS Y PROCEDIMIENTOS DE ADMINISTRACIÓN DE LA CONFIGURACIÓN</td></tr>
<tr><td></td><td colspan="3">La organización deberá desarrollar, diseminar, y periódicamente revisar/actualizar:
(iii) Una política de administración de la configuración formalmente definida y documentada.z
(iv) Procedimientos documentados para facilitar la implantación de la política de administración de la configuración y los controles asociados</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerencia de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">3 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar AI6 – C6</td><td colspan="3">CONFIGURACIÓN BÁSICA</td></tr>
<tr><td></td><td colspan="3">La organización deberá desarrollar, documentar, y mantener actualizada la configuración básica de los Sistemas de Información Computarizados y un inventario de los componentes constitutivos del sistema.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerencia de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">4 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar AI6 – C7</td><td colspan="3">CONFIGURATION SETTINGS</td></tr>
<tr><td></td><td colspan="3">La organización deberá configurar el ambiente de seguridad de los productos de tecnología de información al modo mas restrictivo posible, consistente con los requisitos operacionales de los sistemas de información.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerencia de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">3 meses</td></tr>
<tr><td colspan="4"></td></tr>
</table>

MODELO DE MEJORES PRACTICAS - COBIT			
EMPRESA : Ecuacolor		**Fecha de diagnostico :**	
Diseño de un Sistema de Gestión de Seguridad			Pag 3/3
PLAN DE ACCIÓN			
DOMINIO :	ADQUISICIÓN E IMPLEMENTACIÓN	**PROCESO:**	AI6-Administrar Cambios
Control a Implementar AI6 – C8	**BITÁCORA DE CONTROL DE CAMBIOS**		
	La Gerencia de IT, deberá establecer una bitácora de control de cambios sobre los sistemas de información computarizados.		
Responsables de implementación	Gerencia de Sistemas		
Plazo (tiempo de ejecución)	3 meses		

RIESGOS A MITIGAR

Objetivos de Control	Riesgo Actual			Riesgo Esperado			OBSERVACIÓN
	O	**I**	**T**	**O**	**I**	**T**	
Control de Cambios	7	8	**56**	3	8	**24**	AI6-C7, C1, C8, C6, C5
Distribución de Software	5	8	**40**	1	8	**8**	AI6-C2, C3, C4

MODELO DE MEJORES PRACTICAS - COBIT			
EMPRESA : Ecuacolor	**Fecha de diagnostico :**		
Diseño de un Sistema de Gestión de Seguridad			Pag 1/4
PLAN DE ACCIÓN			
DOMINIO :	ENTREGA Y SOPORTE	**PROCESO:**	DS4 – Asegurar Continuidad del Servicio
que satisface los requerimientos de negocio de:	Asegurar de los servicios de TI estén disponibles de acuerdo con los requerimientos y asegurar un impacto mínimo en el negocio en el evento que ocurra una interrupción mayor.		
se hace posible a través de:	Teniendo un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio.		
y toma en consideración:	• Clasificación con base en la criticidad • Procedimientos alternativos • Respaldo y recuperación • Pruebas y entrenamiento sistemáticos y regulares • Procesos de escalamiento y monitoreo • Responsabilidades organizacionales tanto internas como externas • Planes de reactivación • Actividades de administración de riesgos • Análisis de punto único de falla • Administración de problemas		

CONTROLES	
Control a Implementar DS4 – C1	***POLÍTICAS Y PROCEDIMIENTOS DEL PLAN DE CONTINGENCIA***
	La organización deberá desarrollar, diseminar, y periódicamente revisar/actualizar: (v) Una política del plan de contingencia con el propósito de identificar los roles, responsabilidades y cumplimiento. (vi) Procedimientos documentados para facilitar la implantación de la políticas del plan de continuidad del negocio y los controles asociados
Responsables de implementación	Gerente de Sistemas, Oficial de Seguridad.
Plazo (tiempo de ejecución)	1 mes
Control a Implementar DS4 – C2	**PLAN DE CONTINGENCIA**
	La organización debe desarrollar é implementar un Plan de Contingencia para los sistemas de información . Designar un oficial para que revise y apruebe el plan de contingencia y distribuya copias al personal clave de la contingencia
Responsables de implementación	Gerente de Sistemas, Oficial de Seguridad.
Plazo (tiempo de ejecución)	10 meses
Control a Implementar DS4 – C3	**ENTRENAMIENTO PARA LA CONTINGENCIA**
	La organización debe entrenar al personal involucrado en la contingencia con sus roles , responsabilidades con respecto a los sistemas de información y proveer constantemente entrenamiento . La organización debe incorporar eventos de simulacro dentro del entrenamiento de la contingencia para una respuesta efectiva del personal en situaciones de crisis

Responsables de implementación	Gerente de Sistemas, Oficial de Seguridad.
Plazo (tiempo de ejecución)	2 semanas

MODELO DE MEJORES PRACTICAS - COBIT			
EMPRESA : Ecuacolor		**Fecha de diagnostico :**	
Diseño de un Sistema de Gestión de Seguridad			Pag 2/4
PLAN DE ACCIÓN			
DOMINIO :	ENTREGA Y SOPORTE	**PROCESO:**	DS4 – Asegurar Continuidad del Servicio

Control a Implementar DS4 – C4	**PROBAR EL PLAN DE CONTINGENCIA**
	La organización debe probar el plan de contingencia para los sistemas de información y determinar si el plan es efectivo y la organización está lista para ejecutar el plan
Responsables de implementación	Gerente de Sistemas, Oficial de Seguridad.
Plazo (tiempo de ejecución)	1 mes
Control a Implementar DS4 – C5	**ACTUALIZACIÓN DEL PLAN DE CONTINGENCIA**
	La organización debe revisar el plan de contingencia , los cambios o problemas encontrados durante la implementación , ejecución ó prueba del plan
Responsables de implementación	Gerente de Sistemas, Oficial de Seguridad.
Plazo (tiempo de ejecución)	1 mes
Control a Implementar DS4 – C6	**SITIO ALTERNO DE ALMACENAMIENTO**
	La organización debe identificar un sitio alterno de almacenamiento e iniciar acuerdo necesarios que permitan almacenar la información de respaldo. El sitio debe estar geográficamente bien separado del sitio primario para que o este expuesto a alguna amenaza. El sitio alterno debe estar configurado de manera que sea oportuno y efectivo la recuperación de la información.
Responsables de implementación	Gerente de Sistemas, Oficial de Seguridad.
Plazo (tiempo de ejecución)	1 mes
Control a Implementar DS4 – C7	**SITIO ALTERNO DE PROCESAMIENTO**
	La organización debe identifica el sitio alterno de procesamiento e iniciar los acuerdo necesarios que permita reiniciar las operaciones cuando no este disponible el site primario. El sitio de procesamiento alterno debe estar completamente configurado para soportar el mínimo de capacidad de las operaciones y listo para su uso.
Responsables de implementación	Gerente de Sistemas, Oficial de Seguridad.
Plazo (tiempo de ejecución)	3 mes

MODELO DE MEJORES PRACTICAS - COBIT			
EMPRESA : Ecuacolor		**Fecha de diagnostico :**	
Diseño de un Sistema de Gestión de Seguridad			Pag 3/4
PLAN DE ACCIÓN			
DOMINIO :	ENTREGA Y SOPORTE	**PROCESO:**	DS4 – Asegurar Continuidad del Servicio
Control a Implementar DS4 – C8	**SERVICIO DE TELECOMUNICACIONES**		
	La organización debe tener un servicio alterno de telecomunicaciones cuando el servicio principal de comunicaciones no esté disponible		
Responsables de implementación	Gerente de Sistemas, Oficial de Seguridad.		
Plazo (tiempo de ejecución)	2 semanas		
Control a Implementar DS4 – C9	**BACKUP DE LOS SISTEMAS DE INFORMACIÓN**		
	La organización debe respaldar y almacenar la información en una ubicación apropiadamente segura. Debe almacenar las copias de respaldos del sistema operativo y otros sistemas críticos de información.		
Responsables de implementación	Gerente de Sistemas, Oficial de Seguridad.		
Plazo (tiempo de ejecución)	3 meses		
Control a Implementar DS4 – C10	**RECUPERACIÓN Y RECONSTITUCIÓN DE LOS SISTEMAS DE INFORMACIÓN**		
	La organización debe emplear mecanismos con procedimientos de soporte para permitir que el sistema de información sea recuperado y reconstituido al estado original del sistema después de una interrupción ó falla. La organización debe incluir una recuperación y reconstitución completa del sistema de información como parte de la prueba del plan de contingencia.		
Responsables de implementación	Gerente de Sistemas, Oficial de Seguridad.		
Plazo (tiempo de ejecución)	2 meses		

MODELO DE MEJORES PRACTICAS - COBIT								
EMPRESA : Ecuacolor				**Fecha de diagnostico :**				
Diseño de un Sistema de Gestión de Seguridad								Pag 4/4
PLAN DE ACCIÓN								
DOMINIO :	ENTREGA Y SOPORTE			**PROCESO:**			DS4 – Asegurar Continuidad del Servicio	
RIESGOS A MITIGAR								
Objetivos de Control	**Riesgo Actual**			**Riesgo Esperado**			**OBSERVACIÓN**	
	O	**I**	**T**	**O**	**I**	**T**		
Contenido del Plan de Continuidad de TI	9	10	**90**	3	10	**30**	DS4-C1, C2,	
Mantenimiento del Plan de Continuidad de Tecnología de Información	9	10	**90**	3	10	**30**	DS4-C1,C2, C5	
Pruebas del Plan de Continuidad de TI	9	10	**90**	3	10	**30**	DS4-C1,C2,C4	
Entrenamiento sobre el Plan de Continuidad de Tecnología de Información	9	8	**72**	3	8	**24**	DS4-C1, C2, C3	
Distribución del Plan de Continuidad de TI	9	8	**72**	3	8	**24**	DS4-C1,C2	
Recursos Críticos de Tecnología de Información	9	8	**72**	5	8	**40**	DS4-C1,C2, C10	
Estrategia y Filosofía del Plan de Continuidad de TI	7	8	**56**	4	8	**32**	DS4-C1,C2,C10	
Sitio y Hardware de Respaldo	5	10	**50**	4	10	**40**	DS4-C1,C6,C7,C8	
Almacenamiento de respaldo en el sitio alterno (Off-site)	5	10	**50**	3	10	**30**	DS4-C1, C2, C9	
Procedimiento de afinamiento del Plan de Continuidad	9	6	**54**	5	6	**30**	DS4-C1,C10	

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 1/9</td></tr>
<tr><td colspan="4">PLAN DE ACCIÓN</td></tr>
<tr><td>DOMINIO :</td><td>ENTREGA Y SOPORTE</td><td>PROCESO:</td><td>DS5-Garantizar la seguridad de sistemas</td></tr>
<tr><td>que satisface los requerimientos de negocio de:</td><td colspan="3">Salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida</td></tr>
<tr><td>se hace posible a través de:</td><td colspan="3">Controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados.</td></tr>
<tr><td>y toma en consideración:</td><td colspan="3">• Requerimiento de confidencialidad y privacidad
• Autorización, autenticación y control de acceso
• identificación de usuarios y perfiles de autorización
• Necesidad de tener y necesidad de conocer
• administración de llaves criptográficas
• manejo, reporte y seguimiento de incidentes
• Prevención y detección de virus
• Firewalls
• Administración centralizada de la seguridad
• Entrenamiento de usuarios
• Herramientas para el monitoreo del cumplimiento
• Pruebas y reportes de intrusión</td></tr>
<tr><td colspan="4">CONTROLES</td></tr>
<tr><td>Control a Implementar DS5 – C1</td><td colspan="3">POLÍTICA Y PROCEDIMIENTOS DE CONTROL DE ACCESO</td></tr>
<tr><td></td><td colspan="3">La organización deberá desarrollar, diseminar, y periódicamente revisar/actualizar:
(vii) Una política de control de acceso formalmente definida y documentada.
(viii) Procedimientos documentados para facilitar la implantación de la política de control de acceso y los controles asociados</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerentes de Sistema, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">3 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS5 – C2</td><td colspan="3">REVISIÓN GERENCIAL DE CUENTAS DE USUARIO</td></tr>
<tr><td></td><td colspan="3">La Gerencia deberá contar con un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso. Se debe llevar a cabo la comparación periódica entre los recursos y los registros de las cuentas para reducir el riesgo de errores, fraudes, alteración no autorizada o accidental.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerentes de Sistema, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">1 mes</td></tr>
<tr><td colspan="4"></td></tr>
</table>

<table>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 2/9</td></tr>
<tr><td colspan="4">PLAN DE ACCIÓN</td></tr>
<tr><td>DOMINIO :</td><td>ENTREGA Y SOPORTE</td><td>PROCESO:</td><td>DS5-Garantizar la seguridad de sistemas</td></tr>
<tr><td>Control a Implementar DS5 – C3</td><td colspan="3">UNSUCCESSFUL LOGIN</td></tr>
<tr><td></td><td colspan="3">El sistema de información deberá obligar a un límite de intentos de accesos inválidos consecutivo por un usuario durante un periodo de tiempo. El sistema de información automáticamente deberá bloquear al usuario par un periodo determinado, hasta que se libere el bloqueo por un funcionario con el nivel apropiado.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerentes de Sistema, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">2 semanas</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS5 – C4</td><td colspan="3">ADMINISTRACIÓN DE CUENTAS DE USUARIO</td></tr>
<tr><td></td><td colspan="3">La Gerencia deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la solicitud, establecimiento, emisión, suspensión y cierre 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. La seguridad de acceso a terceros debe definirse contractualmente teniendo en cuenta requerimientos de administración y no revelación.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerentes de Sistema, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">1 mes</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS5 – C5</td><td colspan="3">SUPERVISIÓN Y REVISIÓN DE CONTROL DE ACCESO</td></tr>
<tr><td></td><td colspan="3">La organización deberá supervisar y revisar las actividades de los usuarios con respecto a la aplicación y uso de los controles de accesos a los sistemas de información.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de sistemas, Oficial de Seguridad</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">1 mes</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS5 – C6</td><td colspan="3">ACCESO REMOTO</td></tr>
<tr><td></td><td colspan="3">La organización deberá documentar, monitorear, y controlar todos los métodos de acceso remoto (ej. Dial-up, internet) a los sistemas de información incluyendo el accesos remoto para las funciones</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de sistemas, Oficial de Seguridad</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">3 meses</td></tr>
<tr><td colspan="4"></td></tr>
</table>

<table>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 3/9</td></tr>
<tr><td colspan="4">PLAN DE ACCIÓN</td></tr>
<tr><td>DOMINIO :</td><td>ENTREGA Y SOPORTE</td><td>PROCESO:</td><td>DS5-Garantizar la seguridad de sistemas</td></tr>
<tr><td>Control a Implementar DS5 – C7</td><td colspan="3">CONCIENTIZACION RESPECTO A LA SEGURIDAD IT
(SECURITY AWARENESS)</td></tr>
<tr><td></td><td colspan="3">La organización se asegura a que todos los usuarios (incluyendo gerentes y los altos ejecutivos) estén concientes de la importancia del sistema de seguridad de la información antes de autorizar acceso a los sistemas de información y después de esto.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de sistemas, Oficial de Seguridad</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">2 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS5 – C8</td><td colspan="3">ENTRENAMIENTO DE SEGURIDAD (SECURITY TRAINING)</td></tr>
<tr><td></td><td colspan="3">La organización deberá identificar personal con perfiles y responsabilidades significativos en el SGSI, documentar esos perfiles y responsabilidades, y proporciona apropiado entrenamiento en seguridad de sistema de información antes de autorizar el acceso al sistema y después de esto.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de sistemas, Oficial de Seguridad</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">5 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS5 – C9</td><td colspan="3">REGISTROS DE ENTRENAMIENTO DE SEGURIDAD
(SECURITY TRAINING RECORDS)</td></tr>
<tr><td></td><td colspan="3">La organización deberá documentar y monitorear las actividades de entrenamiento individual de seguridad básico y especifico en los sistemas de información.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de sistemas, Oficial de Seguridad</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">1 mes</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS5 – C10</td><td colspan="3">EVENTOS AUDITABLES (AUDITABLE EVENTS)</td></tr>
<tr><td></td><td colspan="3">El sistema de información debe generar registros de auditoría para los eventos siguientes:
• Inicios de sesión.
• Transacciones que afectan la contabilidad, Inventario, Cxc, CxP, Bancos.
• Altas y Bajas de Maestros de: Cuentas Contables, Proveedores, Clientes, Productos.
• Intentos fallidos de inicio de sesión.</td></tr>
<tr><td>Control a Implementar DS5 – C11</td><td colspan="3">CONTENIDO DE LOS REGISTROS DE AUDITORIA
(CONTENT OF AUDIT RECORDS)</td></tr>
<tr><td></td><td colspan="3">Los Sistemas de Información Computarizados deben capturar suficiente información en los registros de auditoria para establecer que eventos ocurrieron, las fuentes de los eventos, y los resultados de los eventos.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de sistemas, Oficial de Seguridad, Auditor Interno</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">3 meses</td></tr>
</table>

EMPRESA : Ecuacolor		**Fecha de diagnostico :**	
Diseño de un Sistema de Gestión de Seguridad			Pag 4/9
PLAN DE ACCIÓN			
DOMINIO :	ENTREGA Y SOPORTE	**PROCESO:**	DS5-Garantizar la seguridad de sistemas

Control a Implementar DS5 – C12	**CAPACIDAD DE ALMACENAMIENTO PARA LOS LOGS DE AUDITORIA (AUDIT STORAGE CAPACITY)**
	La organización asigna suficiente capacidad de almacenamiento y configura el registro de la auditoria para prevenir que se excede tal espacio.
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad, Auditor Interno
Plazo (tiempo de ejecución)	1 mes
Control a Implementar DS5 – C13	**PROCESAMIENTO DE LA AUDITORIA (AUDIT PROCESSING)**
	En el evento de una falla en el registro de la auditoria o la capacidad de almacenamiento sea alcanzada, el sistema de información alertara apropiadamente a los oficiales de la organización para que tomen las acciones necesarias.
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad, Auditor Interno
Plazo (tiempo de ejecución)	2 meses
Control a Implementar DS5 – C14	**PROTECCIÓN DE LA INFORMACIÓN DE AUDITORIA**
	El Sistema de Información Computarizado protege la información de los LOGS e interfases de auditoria de acceso no autorizado, modificación, y borrado.
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad, Auditor Interno
Plazo (tiempo de ejecución)	1 mes
Control a Implementar DS5 – C15	**RETENCIÓN DE LA INFORMACIÓN DE LOS LOGS DE AUDITORIA (AUDIT RETENTION)**
	La organización retiene los Logs de auditoria por 5 años para proveer apoyo a las investigaciones de después de-el-hecho de incidentes de seguridad y para reunir requerimientos regulatorios y organizacionales de retención de información.
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad, Auditor Interno
Plazo (tiempo de ejecución)	1 mes

EMPRESA : Ecuacolor	Fecha de diagnostico :		
Diseño de un Sistema de Gestión de Seguridad			Pag 5/9
PLAN DE ACCIÓN			
DOMINIO :	ENTREGA Y SOPORTE	**PROCESO:**	DS5-Garantizar la seguridad de sistemas

Control a Implementar DS5 – C16	**CATEGORIZACIÓN DE LA INFORMACIÓN**
	La Gerencia deberá implementar procedimientos para asegurar que todos los datos son clasificados en términos de sensitividad, mediante una decisión explícita y formal del dueño de los datos de acuerdo con el esquema de clasificación de datos. Aún los datos que "no requieren protección" deberán contar con una decisión formal que les asigne dicha clasificación. Los dueños deben determinar la ubicación o disposición de sus datos y determinar quienes pueden compartir los datos aun si y cuando los programas y archivos sean mantenidos, archivados o borrados. Debe quedar evidencia de la aprobación del dueño y de la disposición del dato. Se deben definir políticas para soportar la reclasificación de la información, basados sobre cambios en la sensitividad. El esquema de clasificación debe incluir criterios para administrar el intercambio de información entre organizaciones, teniendo en cuenta tanto la seguridad y el cumplimiento como la legislación relevante.
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad, Auditor Interno
Plazo (tiempo de ejecución)	3 meses
Control a Implementar DS5 – C17	**POLÍTICA Y PROCEDIMIENTOS DE ACREDITACIÓN Y CERTIFICACIÓN**
	La organización deberá desarrollar, diseminar, y periódicamente revisar/actualizar: (ix) Una política de acreditación y certificación formalmente definida y documentada. (x) Procedimientos documentados para facilitar la implantación de la política de acreditación y certificación y los controles asociados
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad, Auditor Interno
Plazo (tiempo de ejecución)	3 meses
Control a Implementar DS5 – C18	**CERTIFICACIÓN DE SEGURIDAD**
	La organización debería dirigir una valoración de los controles de seguridad en los sistemas de información para determinar hasta que punto los controles son implementados correctamente, ejecutados como fueron planeado, y produciendo el resultado deseado con respecto a los requisitos del SGSI.
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad, Auditor Interno
Plazo (tiempo de ejecución)	3 meses

EMPRESA : Ecuacolor	Fecha de diagnostico :

Diseño de un Sistema de Gestión de Seguridad			Pag 6/9
PLAN DE ACCIÓN			
DOMINIO :	ENTREGA Y SOPORTE	**PROCESO:**	DS5-Garantizar la seguridad de sistemas
Control a Implementar DS5 – C19	**PLAN OF ACTION AND MILESTONES**		
	La organización debería desarrolla y actualiza, un plan de acción para el sistema de información que documente los planes de la organización, implementaciones, y evolución de acciones tomadas para remediar cualquier deficiencia notada durante la valoración de los controles de seguridad, para reducir o eliminar vulnerabilidades conocidas.		
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad		
Plazo (tiempo de ejecución)	3 meses		
Control a Implementar DS5 – C20	**ACREDITACIÓN DE SEGURIDAD**		
	La organización debería autorizar (es decir, acreditar) a los sistema de información antes de empezar a funcionar y cada cierto tiempo. El oficial de seguridad debería firmar y aprobar la acreditación de seguridad		
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad, Auditor Interno		
Plazo (tiempo de ejecución)	2 meses		
Control a Implementar DS5 – C21	**MONITOREO CONTINUO**		
	La organización debería supervisar que los controles de seguridad en los sistema de información se mantengan de una forma continua.		
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad, Auditor Interno		
Plazo (tiempo de ejecución)	3 meses		
Control a Implementar DS5 – C22	**POLÍTICA Y PROCEDIMIENTOS DE RESPUESTA A INCIDENTES**		
	La organización deberá desarrollar, diseminar, y periódicamente revisar/actualizar: (xi) Una política de respuesta a incidentes formalmente definida y documentada. (xii) Procedimientos documentados para facilitar la implantación de la política de respuesta a incidentes y los controles asociados		
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad, Auditor Interno		
Plazo (tiempo de ejecución)	3 meses		
Control a Implementar DS5 – C23	**MANEJO DE INCIDENTES (INCIDENT HANDLING)**		
	La organización debería implementar una actividad de manejo de incidentes para los eventos de seguridad y debería incluir: preparación, detección y análisis, contención, erradicación, y recuperación.		
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad, Auditor Interno		
Plazo (tiempo de ejecución)	3 meses		
EMPRESA : Ecuacolor	**Fecha de diagnostico :**		

<table>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 7/9</td></tr>
<tr><td colspan="4">PLAN DE ACCIÓN</td></tr>
<tr><td>DOMINIO :</td><td>ENTREGA Y SOPORTE</td><td>PROCESO:</td><td>DS5-Garantizar la seguridad de sistemas</td></tr>
<tr><td>Control a Implementar
DS5 – C24</td><td colspan="3">REPORTES DE VIOLACIÓN Y DE ACTIVIDADES DE SEGURIDAD</td></tr>
<tr><td></td><td colspan="3">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 logs) deberá otorgarse tomando como base el principio de menor privilegio o necesidad de saber.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de sistemas, Oficial de Seguridad</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">3 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar
DS5 – C25</td><td colspan="3">INCIDENT REPORTING</td></tr>
<tr><td></td><td colspan="3">La organización debería reportar rápidamente los informes de incidentes a las autoridades apropiadas.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de sistemas, Oficial de Seguridad</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">1 mes</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar
DS5 – C26</td><td colspan="3">INCIDENT RESPONSE ASSISTANCE</td></tr>
<tr><td></td><td colspan="3">La organización debería proporcionar ayuda a los usuarios de los sistemas de información para el manejo e información de los incidentes de seguridad.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de sistemas, Oficial de Seguridad</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">3 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar
DS5 – C27</td><td colspan="3">POLÍTICA Y PROCEDIMIENTOS PARA LA PLANIFICACIÓN DE LA SEGURIDAD</td></tr>
<tr><td></td><td colspan="3">La organización deberá desarrollar, diseminar, y periódicamente revisar/actualizar:
(i) Una política para la planificación de seguridad formalmente definida y documentada.
(ii) Procedimientos documentados para facilitar la implantación de la política de la planificación de la seguridad y los controles asociados</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de sistemas, Oficial de Seguridad, Auditor Interno</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">5 meses</td></tr>
</table>

EMPRESA : Ecuacolor	**Fecha de diagnostico :**	
Diseño de un Sistema de Gestión de Seguridad		Pag 8/9
PLAN DE ACCIÓN		

DOMINIO :	ENTREGA Y SOPORTE	**PROCESO:**	DS5-Garantizar la seguridad de sistemas

Control a Implementar DS5 – C28	**PLAN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN**
	La organización debería desarrollar e implementar un plan de seguridad para los sistema de información que proporciona una apreciación global de los requisitos de seguridad para los sistemas y una descripción de la controles de seguridad que existen o están planeados implantar.
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad
Plazo (tiempo de ejecución)	3 meses
Control a Implementar DS5 – C29	**ACTUALIZAR PLAN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN**
	La organización debería revisar el plan de seguridad para los sistemas de información, para detectar cualquier desviación o efectuar alguna corrección.
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad
Plazo (tiempo de ejecución)	3 meses
Control a Implementar DS5 – C30	**REGLAS DE CONDUCTA**
	La organización debería establecer y hacer prontamente disponible a todos los usuarios de los sistemas de información un juego de reglas que describen sus responsabilidades y conducta esperada con respecto a los usos de los sistemas de información. La organización debería recibir firmado el reconocimiento de los usuarios en donde se indica que ellos han leído, han entendido, y han estado de acuerdo en someterse a las reglas de conducta, antes de autorizar el acceso a los sistemas de información.
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad
Plazo (tiempo de ejecución)	3 meses
Control a Implementar DS5 – C31	**CONTROL DE LOS USUARIOS SOBRE SUS CUENTAS**
	Los usuarios deberán controlar en forma sistemática la actividad de su(s) propia(s) cuenta (s). También se deberán establecer mecanismos de información para permitirles supervisar la actividad normal, así como alertarlos oportunamente sobre actividades inusuales.
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad
Plazo (tiempo de ejecución)	3 meses

EMPRESA : Ecuacolor	**Fecha de diagnostico :**

Diseño de un Sistema de Gestión de Seguridad			Pag 9/9
PLAN DE ACCIÓN			
DOMINIO :	ENTREGA Y SOPORTE	**PROCESO:**	DS5-Garantizar la seguridad de sistemas
Control a Implementar DS5 – C32	**PLAN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN**		
	La organización debería desarrollar e implementar un plan de seguridad para los sistema de información que proporciona una apreciación global de los requisitos de seguridad para los sistemas y una descripción de la controles de seguridad que existen o están planeados implantar.		
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad		
Plazo (tiempo de ejecución)	3 meses		
Control a Implementar DS5 – C33	**VIGILANCIA DE SEGURIDAD**		
	La administración de seguridad de TI debe asegurar que la actividad de seguridad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente a todos aquellos que puedan verse afectados, tanto interna como externamente y se debe actuar de una manera oportuna.		
Responsables de implementación	Gerente de sistemas, Oficial de Seguridad		
Plazo (tiempo de ejecución)	3 meses		

RIESGOS A MITIGAR

Objetivos de Control	Riesgo Actual			Riesgo Esperado			OBSERVACIÓN
	O	I	T	O	I	T	
Administrar Medidas de Seguridad	9	8	**72**	5	8	**40**	DS5-C1, C7, C8, C9, C19, C20, C21, C27, C28, C29, C30, C32
Administración de Cuentas de Usuario	5	8	**40**	3	8	**24**	DS5-C1, C3, C4, C5, C6, C7, C8
Revisión Gerencial de Cuentas de Usuario	7	6	**42**	5	6	**30**	DS5-C2, C5, C6
Control de Usuarios sobre Cuentas de Usuario	7	8	**56**	5	8	**40**	DS5-C7, C31
Vigilancia de Seguridad	7	8	**56**	3	8	**24**	DS5-C10, C11, C12, C13, C14, C15, C33
Clasificación de Datos	7	6	**42**	5	6	**30**	DS5-C16
Reportes de Violación y de Actividades de Seguridad	7	8	**56**	3	8	**24**	DS5-C10, C11, C12, C13, C14, C15, C24
Manejo de Incidentes	5	8	**40**	3	8	**24**	DS5-C22, C23, C24, C25, C26
Reacreditación	9	4	**36**	7	4	**28**	DS5-C17, C18, C20, C21

MODELO DE MEJORES PRACTICAS – COBIT			
EMPRESA : Ecuacolor		**Fecha de diagnostico :**	
Diseño de un Sistema de Gestión de Seguridad			Pag 1/3
PLAN DE ACCIÓN			
DOMINIO :	ADQUISICIÓN E IMPLEMENTACIÓN	**PROCESO:**	DS11-Administrar los Datos
que satisface los requerimientos de negocio de:	Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento		
se hace posible a través de:	Una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI		
y toma en consideración:	• Diseño de formatos • Controles de documentos fuente • Controles de entrada, procesamiento y salida • Identificación, movimiento y administración de la librería de medios • Recuperación y respaldo de datos • Autenticación e integridad • Propiedad de datos • Políticas de administración de datos • Modelo de datos y estándares de representación de datos • Integración y consistencia a través de plataformas • Requerimientos legales y regulatorios		
CONTROLES			
Control a Implementar DS11 – C1	**POLÍTICAS Y PROCEDIMIENTOS DE ADMINISTRACIÓN DE DATOS**		
	La Organización deberá diseñar, implementar y periódicamente revisar/actualizar: • Flujo de datos dentro de la función de TI y hacia/desde los usuarios de los datos • Proceso de autorización de documentos fuente • Procesos de recolección, seguimiento y transmisión de datos • Procedimientos utilizados para identificar y corregir errores durante la creación de datos • Métodos utilizados por la organización para retener documentos fuente (archivo, imágenes, etc.), para definir qué documentos deben ser retenidos, los requerimientos de retención legales y regulatorios, etc. • Contratos de proveedores para llevar a cabo tareas de administración de datos • Reportes administrativos utilizados para monitorear actividades e inventarios		
Responsables de implementación	Gerencia de Sistemas		
Plazo (tiempo de ejecución)	8 meses		

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS – COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 2/3</td></tr>
<tr><td colspan="4">PLAN DE ACCIÓN</td></tr>
<tr><td>DOMINIO :</td><td>ADQUISICIÓN E IMPLEMENTACIÓN</td><td>PROCESO:</td><td>DS11-Administrar los Datos</td></tr>
<tr><td colspan="4">CONTROLES</td></tr>
<tr><td>Control a Implementar DS11 – C2</td><td colspan="3">REVISIÓN DE TODAS LAS APLICACIONES CRÍTICAS</td></tr>
<tr><td></td><td colspan="3">La Gerencia de IT deberá revisar:
• Módulos que lleven a cabo revisiones de precisión, suficiencia y autorización de captura en el ingreso de datos
• Funciones que lleven a cabo entradas de datos para cada aplicación
• Funciones que lleven a cabo rutinas de corrección de errores de entrada de datos
• Métodos utilizados para prevenir (por medios manuales y programados), detectar y corregir errores
• Control de la integridad de los procesos de datos enviados a proceso
• Distribución de salidas sensitiva sólo a personas autorizadas
• Procedimientos de balanceo de salidas para control de totales y conciliación de variaciones</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerencia de Sistemas</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">7 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS11 – C3</td><td colspan="3">POLÍTICAS Y PROCEDIMIENTOS DE REPOSITORIO CENTRAL DE BASES DE DATOS</td></tr>
<tr><td></td><td colspan="3">La organización deberá establecer las normas, diseño y control:
• Organización de la base de datos y diccionario de datos
• Procedimientos de mantenimiento y seguridad de bases de datos
• Determinación y mantenimiento de la propiedad de las bases de datos
• Procedimientos de control de cambios sobre el diseño y contenido de la base de datos
• Reportes administrativos y pistas de auditoría que definen actividades de bases de datos</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerencia de Sistemas</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">6 meses</td></tr>
<tr><td colspan="4"></td></tr>
</table>

MODELO DE MEJORES PRACTICAS – COBIT			
EMPRESA : Ecuacolor		**Fecha de diagnostico :**	
Diseño de un Sistema de Gestión de Seguridad			Pag 3/3
PLAN DE ACCIÓN			
DOMINIO :	ADQUISICIÓN E IMPLEMENTACIÓN	**PROCESO:**	DS11-Administrar los Datos
Control a Implementar DS11 – C4	**POLÍTICAS Y PROCEDIMIENTOS DE LIBRERÍA DE MEDIOS Y ALMACENAMIENTO DE DATOS EXTERNO**		
	La organización deberá definir los controles para: • Administración de la librería de medios y del sistema de administración de la librería • Requerir la identificación externa de todos los medios • Requerir el inventario actual de todos los contenidos y procesos para actividades de control • Procedimientos de reconciliación entre registros actuales y registros de datos almacenados • Reciclaje de datos y protección de información sensitiva • Rotación de medios de datos • Inventario de datos de prueba y pruebas de recuperación llevadas a cabo • Medios y funciones del personal en el sitio alterno en el plan de continuidad • Asegurar que el archivo cumple con requerimientos legales y de negocio		
Responsables de implementación	Gerencia de Sistemas		
Plazo (tiempo de ejecución)	3 meses		

RIESGOS A MITIGAR

Objetivos de Control	**Riesgo Actual**			**Riesgo Esperado**			**OBSERVACIÓN**
	O	**I**	**T**	**O**	**I**	**T**	
Chequeos de Exactitud, Suficiencia y Autorización	7	8	**56**	3	8	**24**	DS11-C1, C2, C3
Integridad de Procesamiento de Datos	5	8	**40**	3	8	**24**	DS11-C2, C3, C4
Provisiones de Seguridad para Reportes de Salida	7	8	**56**	2	8	**16**	DS11-C2
Protección de Información Sensible durante transmisión y transporte	7	8	**56**	3	8	**24**	DS11-C1
Protección de Información Sensitiva Desechada	7	6	**42**	3	6	**18**	DS11-C4
Sistema de Administración de la Librería de Medios	7	8	**56**	2	8	**16**	DS11-C3, C4
Archivo	7	6	**42**	3	6	**18**	DS11-C4

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 1/5</td></tr>
<tr><td colspan="4">PLAN DE ACCIÓN</td></tr>
<tr><td>DOMINIO :</td><td>ENTREGA Y SOPORTE</td><td>PROCESO:</td><td>DS12 - Administrar las instalaciones</td></tr>
<tr><td>que satisface los requerimientos de negocio de:</td><td colspan="3">Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales o fallas humanas.</td></tr>
<tr><td>se hace posible a través de:</td><td colspan="3">La instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado.</td></tr>
<tr><td>y toma en consideración:</td><td colspan="3">• acceso a instalaciones
• identificación del sitio
• seguridad física
• Políticas de inspección y escalamiento
• Planeación de continuidad del negocio y administración de crisis
• salud y seguridad del personal
• Políticas de mantenimiento preventivo
• protección contra amenazas ambientales
• Monitoreo automatizado</td></tr>
<tr><td colspan="4">CONTROLES</td></tr>
<tr><td>Control a Implementar DS12 – C1</td><td colspan="3">POLÍTICAS Y PROCEDIMIENTOS DE MANTENIMIENTO DE SISTEMAS</td></tr>
<tr><td></td><td colspan="3">La organización deberá desarrollar, diseminar, y periódicamente revisar/actualizar:
(xiii) Una política de mantenimiento de sistemas formalmente definida y documentada.
(xiv) Procedimientos documentados para facilitar la implantación de la política de mantenimiento de sistemas y los controles asociados.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">1 mes</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS12 – C2</td><td colspan="3">MANTENIMIENTO PERIÓDICO</td></tr>
<tr><td></td><td colspan="3">La organización deberá fijar, realizar, y documentar el preventivo, rutinario y regular mantenimiento en los componentes de los sistemas de información de acuerdo con las especificaciones del fabricante o vendedor y/o las de los requerimientos internos.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">2 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS12 – C3</td><td colspan="3">PERSONAL DE MANTENIMIENTO</td></tr>
<tr><td></td><td colspan="3">La organización deberá mantener una lista de personal autorizado para realizar mantenimiento sobre el sistema de información. Sólo personal autorizado debería realizar mantenimiento en el sistema de información.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">2 semanas</td></tr>
</table>

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3"><code>Diseño de un Sistema de Gestión de Seguridad</code></td><td>Pag 2/5</td></tr>
<tr><td colspan="4">PLAN DE ACCIÓN</td></tr>
<tr><td>DOMINIO :</td><td>ENTREGA Y SOPORTE</td><td>PROCESO:</td><td>DS12 - Administrar las instalaciones</td></tr>
<tr><td>Control a Implementar DS12 – C4</td><td colspan="3">POLÍTICAS Y PROCEDIMIENTOS DE PROTECCIÓN DE MEDIOS.</td></tr>
<tr><td></td><td colspan="3">La organización deberá desarrollar, diseminar, y periódicamente revisar/actualizar:
(xv) Una política de protección de medios formalmente definida y documentada.
(xvi) Procedimientos documentados para facilitar la implantación de la política de protección de medios y los controles asociados.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">1 mes</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS12 – C5</td><td colspan="3">ACCESO A MEDIOS (MEDIA ACCESS)</td></tr>
<tr><td></td><td colspan="3">La organización deberá asegurar que sólo los usuarios autorizados tienen acceso a información en forma impresa o en medios de comunicación digitales extraídos de los sistemas de información.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">1 mes</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS12 – C6</td><td colspan="3">DESTRUCCIÓN Y DISPOSICIÓN DE MEDIOS
(MEDIA DESTRUCTION AND DISPOSAL)</td></tr>
<tr><td></td><td colspan="3">La organización deberá sanear o destruir los medios digitales de los sistemas de información antes de su disposición o descargo, para reutilizar fuera de la organización, para prevenir que individuos no autorizados puedan obtener acceso y usar la información contenida en estos.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">1 mes</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS12 – C7</td><td colspan="3">POLÍTICAS Y PROCEDIMIENTOS DE PROTECCIÓN AMBIENTAL Y FÍSICA.</td></tr>
<tr><td></td><td colspan="3">La organización deberá desarrollar, diseminar, y periódicamente revisar/actualizar:
(xvii) Una política de protección de ambiental y física formalmente definida y documentada.
(xviii) Procedimientos documentados para facilitar la implantación de la política de protección ambiental y física y los controles asociados.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">1 mes</td></tr>
<tr><td colspan="4"></td></tr>
</table>

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 3/5</td></tr>
<tr><td colspan="4">PLAN DE ACCIÓN</td></tr>
<tr><td>DOMINIO :</td><td>ENTREGA Y SOPORTE</td><td>PROCESO:</td><td>DS12 - Administrar las instalaciones</td></tr>
<tr><td>Control a Implementar DS12 – C8</td><td colspan="3">AUTORIZACIONES DE ACCESO FÍSICO</td></tr>
<tr><td></td><td colspan="3">La organización deberá desarrollar y conservar listas actualizadas del personal con acceso autorizado a los recursos de los sistemas de información y deberán portar credenciales apropiadas de autorización (ej., insignias, tarjetas de identificación). El oficial de seguridad debe revisar y aprobar la lista de acceso y la autorización de credenciales.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">2 semanas</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS12 – C9</td><td colspan="3">CONTROL DE ACCESO FÍSICO</td></tr>
<tr><td></td><td colspan="3">La organización deberá controlar todos los puntos de acceso físico a los recursos de los sistemas de información y verificar autorizaciones de acceso individuales antes de conceder acceso a los recursos. La organización también deberá controlar el acceso a las áreas oficialmente designadas como públicamente accesible, como es apropiado, en acuerdo con la valoración de riesgos de la organización.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">3 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS12 – C10</td><td colspan="3">MONITOREAR EL ACCESO FÍSICO</td></tr>
<tr><td></td><td colspan="3">La organización deberá monitorear el acceso físico a los sistemas de información para detectar y responder a incidentes.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">2 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS12 – C11</td><td colspan="3">CONTROL DE VISITANTES</td></tr>
<tr><td></td><td colspan="3">La organización deberá controlar el acceso físico a los sistemas de información autenticando a los visitantes antes de autorizar acceso a los recursos.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">2 meses</td></tr>
<tr><td colspan="4"></td></tr>
</table>

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 4/5</td></tr>
<tr><td colspan="4">PLAN DE ACCIÓN</td></tr>
<tr><td>DOMINIO :</td><td>ENTREGA Y SOPORTE</td><td>PROCESO:</td><td>DS12 - Administrar las instalaciones</td></tr>
<tr><td>Control a Implementar DS12 – C12</td><td colspan="3">ESCOLTA DE VISITANTES</td></tr>
<tr><td></td><td colspan="3">Deberán establecerse procedimientos apropiados que aseguren que las personas que no formen parte del grupo de operaciones de la función de servicios de información sean escoltadas por algún miembro de ese grupo cuando deban entrar a las instalaciones de cómputo. Deberá mantenerse y revisarse regularmente una bitácora de visitantes.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">1 mes</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS12 – C13</td><td colspan="3">BITÁCORA DE VISITANTES</td></tr>
<tr><td></td><td colspan="3">La organización deberá mantener una bitácora de visitantes que incluye:
(i) el nombre y organización del persona que visita;
(ii) la firma de el visitante;
(iii) la forma de identificación;
(iv) la fecha de acceso;
(v) tiempo de entrada y salida;
(vi) propósito de visita; y
(vii) el nombre y organización de la persona visitada.
El Oficial de Seguridad revisara regularmente la bitácora.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">2 semanas</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS12 – C14</td><td colspan="3">LUCES DE EMERGENCIA</td></tr>
<tr><td></td><td colspan="3">La organización deberá emplear y mantener un sistema automático de luces de emergencia que se activan al evento de un fallo de poder o ruptura y que cubre salidas de emergencia y rutas de evacuación.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerencia General, Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">7 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS12 – C15</td><td colspan="3">PROTECCIÓN CONTRA INCENDIOS</td></tr>
<tr><td></td><td colspan="3">La organización deberá emplear y mantener un sistema automático de luces de emergencia que se activan al evento de un fallo de poder o ruptura y que cubre salidas de emergencia y rutas de evacuación.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerencia General, Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">7 meses</td></tr>
<tr><td colspan="4"></td></tr>
</table>

<table>
<tr><td colspan="4">MODELO DE MEJORES PRACTICAS - COBIT</td></tr>
<tr><td colspan="2">EMPRESA : Ecuacolor</td><td colspan="2">Fecha de diagnostico :</td></tr>
<tr><td colspan="3">Diseño de un Sistema de Gestión de Seguridad</td><td>Pag 5/5</td></tr>
<tr><td colspan="4">PLAN DE ACCIÓN</td></tr>
<tr><td>DOMINIO :</td><td>ENTREGA Y SOPORTE</td><td>PROCESO:</td><td>DS12 - Administrar las instalaciones</td></tr>
<tr><td>Control a Implementar DS12 – C16</td><td colspan="3">CONTROLES DE TEMPERATURA Y HUMEDAD</td></tr>
<tr><td></td><td colspan="3">La organización deberá monitorear la temperatura y humedad, y mantener regularmente dentro de los niveles aceptables las instalaciones de Tecnología.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerencia General, Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">8 meses</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS12 – C17</td><td colspan="3">PROTECCIÓN CONTRA DAÑOS OCASIONADOS POR EL AGUA</td></tr>
<tr><td></td><td colspan="3">La organización deberá proteger el sistema de información de daño de agua que resulta de la ruptura líneas de plomería u otras fuentes de goteo de agua asegurando que las válvulas maestras de "shutoff" son accesibles, funcionan apropiadamente, y son conocidas por el personal principal.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerente General, Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">2 semanas</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Control a Implementar DS12 – C18</td><td colspan="3">DISCRECIÓN SOBRE LAS INSTALACIONES DE TECNOLOGÍA DE INFORMACIÓN</td></tr>
<tr><td></td><td colspan="3">La Gerencia de la función de servicios de información deberá asegurar que se mantenga un bajo perfil sobre la identificación física de las instalaciones relacionadas con sus operaciones de tecnología de información. La información sobre la ubicación del sitio debe ser limitada y mantenerse con la adecuada reserva.</td></tr>
<tr><td>Responsables de implementación</td><td colspan="3">Gerencia General, Gerente de Sistemas, Oficial de Seguridad.</td></tr>
<tr><td>Plazo (tiempo de ejecución)</td><td colspan="3">8 meses</td></tr>
</table>

<table>
<tr><td colspan="8">RIESGOS A MITIGAR</td></tr>
<tr><td rowspan="2">Objetivos de Control</td><td colspan="3">Riesgo Actual</td><td colspan="3">Riesgo Esperado</td><td rowspan="2">OBSERVACIÓN</td></tr>
<tr><td>O</td><td>I</td><td>T</td><td>O</td><td>I</td><td>T</td></tr>
<tr><td>Seguridad Física</td><td>7</td><td>10</td><td>70</td><td>5</td><td>10</td><td>50</td><td>DS12-C1, C2, C3, C4, C5, C6, C9, C10</td></tr>
<tr><td>Discreción sobre las Instalaciones de Tecnología de Información</td><td>7</td><td>6</td><td>42</td><td>5</td><td>6</td><td>30</td><td>DS12-C3, C5, C18</td></tr>
<tr><td>Escolta de Visitantes</td><td>9</td><td>6</td><td>54</td><td>3</td><td>6</td><td>18</td><td>DS12-C8, C9, C10, C11, C12, C13</td></tr>
<tr><td>Protección contra Factores Ambientales</td><td>7</td><td>6</td><td>42</td><td>5</td><td>6</td><td>30</td><td>DS12-C7, C14, C15, C16, C17</td></tr>
</table>

9 BENEFICIOS

La implantación de un Sistema de Gestión de la Seguridad de la Información proporciona a Ecuacolor Laboratorio Fotográfico los siguientes beneficios:

- Un análisis de riesgos de sus Sistemas de Información.
- Una gestión adecuada de los riesgos según su modelo de empresa.
- Una mejora continua de su gestión de la seguridad.
- El cumplimento de la legislación vigente sobre protección de datos de carácter personal, comercio electrónico, propiedad intelectual, etc.
- Facilita el logro de los objetivos de la organización.
- Hace a la organización más segura y consciente de sus riesgos.
- Mejoramiento continúo del Sistema de Control Interno.
- Optimiza la asignación de recursos.
- Aprovechamiento de oportunidades de negocio.
- Fortalece la cultura de autocontrol.
- Mayor estabilidad ante cambios del entorno.
- Conocer y Analizar sus riesgos, identificando amenazas, vulnerabilidades e impactos en su empresa.
- Reducir eficazmente el nivel de riesgo mediante los controles adecuados
- Organizar los recursos de la seguridad.
- Integra la Gestión de la Seguridad SI.
- Aporta confianza a los sistemas de información

Y en definitiva, establece una cultura de la seguridad y una excelencia en el tratamiento de la información en todos sus procesos de negocio. Así, aporta un valor añadido de reconocido prestigio, en la calidad de los servicios que ofrece a sus clientes.