**1 WHAT IS INFORMATION SECURITY**

**1.1 HOW TO ESTABLISH SECURITY REQUIREMENTS**

**1.2 What is a Information security policy document**

**1.3 ASSESSING SECURITY RISKS**

**1.4 SELECTING CONTROLS**

**2 ISO 27002-27005**

**2.1 SECURITY POLICY :**

El Documento de la Política de Seguridad de la Información debe contar con un claro lineamiento de implementación, y debe contener partes tales como una definición de seguridad de la información, sus objetivos y alcances generales, importancia, intención de la gerencia en cuanto al tema de seguridad de la información, estructuras de evaluación y [gestión de riesgos](http://www.monografias.com/trabajos29/auditoria-seguridad/auditoria-seguridad.shtml), explicación de las políticas o [principios](http://www.monografias.com/trabajos6/etic/etic.shtml) de la organización, definición de las responsabilidades individuales en cuanto a la seguridad, etc.

**2.1.1 Information security policy document**

o La relación con la política general del negocio:

Cumplir con los términos acordados con los clientes

o Documentación de la política de seguridad de la información.

No existen.

o Política de seguridad.

No están escritas, no hay documentos.

**2.2 ORGANIZATION OF INFORMATION SECURITY:**

La organización de la seguridad de la información se puede dar de dos formas: organización interna y organización con respecto a terceros.

En cuanto a la organización interna, se tiene como objetivo manejar la seguridad de la información dentro de la organización.

Deben también existir acuerdos de confidencialidad.

Es fundamental también asignar responsabilidades.

También se debe tener en cuenta mantener los contactos apropiados con las autoridades relevantes

La organización en materia de seguridad de la información debe también considerarse respecto a terceros.

Para ello se debe comenzar por la identificación de los riesgos relacionados con los grupos externos.

**2.2.1 Allocation of information security responsibilities**

o Organización de la seguridad de la información.

No Hay una estructura como tal.

**2.3 ASSET MANAGEMENT**

Se deben asignar responsabilidades por cada uno de los activos de la organización, así como poseer un [inventario](http://www.monografias.com/trabajos11/conin/conin.shtml) actualizado de todos los activos que se tienen, a quien/quienes les pertenecen, el uso que se les debe dar, y la clasificación de todos los activos. Para esto el departamento de [contabilidad](http://www.monografias.com/Administracion_y_Finanzas/Contabilidad/) tendrá que hacer un buen trabajo en cuanto a esta clasificación y desglose de activos, y el departamento de leyes de la empresa también tendrá que ser muy metódico en estos procesos, ya que los activos son todos los [bienes](http://www.monografias.com/trabajos16/configuraciones-productivas/configuraciones-productivas.shtml) y recursos que posee una empresa, incluyendo bienes muebles e inmuebles, [dinero](http://www.monografias.com/trabajos16/marx-y-dinero/marx-y-dinero.shtml), etc.

**2.3.1 Inventory of assets**

o Los recursos necesarios: software, hardware y personal.

**2.3.2 Ownership of assets**

o Seguridad de los RRHH. Gestión de activos.

Si, la administración de los activos se realiza dentro del CRM.

**2.3.3 Acceptable use of asset**

**2.4 HUMAN RESOURCES SECURITY**

El objetivo de esto es asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados, reduciendo el [riesgo](http://www.monografias.com/trabajos13/ripa/ripa.shtml) de robo, [fraude](http://www.monografias.com/trabajos11/fraer/fraer.shtml#fra) y mal uso de los medios. Es necesario definir claramente los roles y responsabilidades de cada empleado. Todo esto no debe ser simplemente mediante acuerdos verbales, sino que se debe plasmar en el contrato de trabajo.

o Asignación de responsabilidades.

**2.4.1 Roles and responsibilities**

o La estructura y responsables del proceso de Gestión de la Seguridad.

Gerente de Operaciones y de planta.

o Los responsables de cada subproceso.

Jefe de planta : Incidentes dentro de la planta y de mantenimiento.

Atención a clientes: Coordinadora de atención a clientes.

Obreros : Todo lo que concierne a la mano de obra.

COO: Encargado de la seguridad de la planta y de las demás áreas

**2.4.2 Terms and conditions of employment**

o Cumplimiento con requerimientos legales y contractuales

Obligaciones legales: \*

\* Con el gobierno hay que cumplir con requerimientos de impuestos, permisos para compra y ventas que van dentro del marco que manifiestas a la hora de crear la empresa.

\*Con la secretaria de trabajo, no fallar con el reglamento de seguridad.

\*Con la sociedad, con el ambiente hablando de los contaminantes.

Contractuales:

COn clientes

Con trabajadores

Con proveedores

**2.4.3 Information security awareness, education, and training**

o Los programas de formación.

Capacitación para la operación de la maquinaria disponible a nivel obrero.

o Concienciación, formación y capacitación en seguridad de la información.

No hay.

**2.4.4 Disciplinary process**

o Los procesos y procedimientos empleados.

**2.5 PHYSICAL AND ENVIRONMENTAL SECURITY**

La seguridad física y ambiental se divide en *áreas seguras* y *seguridad de los equipos.* Respecto a las áreas seguras, se refiere a un perímetro de seguridad física que cuente con barreras o [límites](http://www.monografias.com/trabajos6/lide/lide.shtml) .Se debe también contar con controles físicos de entrada, tales como puertas con llave, etc. Además de eso, es necesario considerar la seguridad física con respecto a amenazas externas y de origen ambiental.Deben también haber áreas de acceso público de carga y descarga, parqueos, áreas de visita, entre otros

En cuanto a la seguridad ambiental, se debe controlar la [temperatura](http://www.monografias.com/trabajos/termodinamica/termodinamica.shtml) adecuada para los equipos, seguridad del cableado, mantenimiento de equipos, etc. Para todo esto se requerirá de los [servicios](http://www.monografias.com/trabajos14/verific-servicios/verific-servicios.shtml) de técnicos o ingenieros especializados en el cuidado y mantenimiento de cada uno de los equipos, así como en la inmediata reparación de los mismos cuando sea necesario. La ubicación de los equipos también debe ser adecuada y de tal manera que evite riesgos.

Se debe igualmente verificar y controlar el [tiempo](http://www.monografias.com/trabajos901/evolucion-historica-concepciones-tiempo/evolucion-historica-concepciones-tiempo.shtml) de vida útil de los equipos para que trabajen en condiciones óptimas.

**2.5.1 Physical entry controls**

o Seguridad física y ambiental.

La seguridad física la proporciona el dueño del edificio.Pertenecen a un condominio de varias empresas.

**2.5.2 Protecting against external and environmental threats**

**2.5.3 Working in secure areas**

**2.5.4 Equipment maintenance**

**2.6 COMMUNICATIONS AND OPERATIONS MANAGEMENT**

En primer lugar, es necesario que los procedimientos de operación estén bien documentados, pues no basta con tener las ideas en la mente de los administradores, sino que se deben plasmar en [documentos](http://www.monografias.com/trabajos14/comer/comer.shtml) que por supuesto estén autorizados por la gerencia.

Otro aspecto fundamental es la gestión de cambios. Un cambio relevante no se debe hacer jamás sin documentarlo,Se debe tener cuidado que nadie pueda tener acceso, modificar o utilizar los activos sin autorización o detección

Se tienen que establecer políticas, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de [comunicación](http://www.monografias.com/trabajos12/fundteo/fundteo.shtml).

**2.6.1 Documented operating procedures**

o La coordinación con los otros procesos TI.

o Seguridad en las operaciones.

SI, normas de la seguridad para los trabajadores , para el manejo de equipos, de residuos peligrosos, uniformes y ropa de seguridad.

**2.6.2 Monitoring and review of third party services**

o El nivel de monitorización de la seguridad.

El encargado de IT y el Gerente de Operaciones.

**2.6.3 Capacity management**

**2.6.4 Controls against malicious code**

**2.6.5 Information back-up**

**2.6.6 Network controls**

**2.6.7 Information exchange policies and procedures**

o Transferencia de información.

**2.7 ACCESS CONTROL**

Todo acceso no autorizado debe ser evitado y se deben minimizar al máximo las probabilidades de que eso suceda. Todo esto se controla mediante [registro](http://www.monografias.com/trabajos7/regi/regi.shtml) de usuarios, gestión de privilegios, autenticación mediante usuarios y contraseñas, etc.

Aparte de la autenticación correspondiente, los usuarios deben asegurar que el equipo desatendido tenga la protección apropiada.Son necesarios controles de acceso a la red, al sistema operativo, a las aplicaciones y a la información. Para todo esto deben existir [registros](http://www.monografias.com/trabajos7/regi/regi.shtml) y bitácoras de acceso.

**2.7.1 Access control policy**

o Los protocolos de acceso a la información.

Hay personal con perfiles definidos, cada perfil tiene sus respectivos niveles de acceso.

Los roles se dividen por departamentos tales como: Recursos humanos, Ventas, Compras y Producción.

No existen protocolos específicos.

**2.7.2 Privilege management**

o Control de accesos.

Si ,hay perfiles.

**2.7.3 Teleworking**

**2.8 INFORMATION SECURITY INCIDENT MANAGEMENT**

La comunicación es fundamental en todo proceso. Por lo tanto, se debe trabajar con reportes de los eventos y debilidades de la seguridad de la información, asegurando una comunicación tal que permita que se realice una acción correctiva oportuna, llevando la información a través de los canales gerenciales apropiados lo más rápidamente posible.

**2.8.1 Reporting Information Security Events and Weaknesses**

o Los procedimientos de análisis de riesgos.

No hay algun documento donde se escriban los procedimientos en caso de riesgos.

o Qué informes deben ser emitidos periódicamente.

Los financieros como el estado de resultados y balances, indicadores de ventas , desempeño de los sistemas informáticos, de mantenimiento y calidad.

**2.8.2 Responsibilities and procedures**

o El alcance del Plan de Seguridad.

No hay.

o Gestión de los incidentes de seguridad.

No hay protocolos.

**2.9 BUSINESS CONTINUITY MANAGEMENT**

Se debe contar con planes de continuidad del negocio que incluyan la seguridad de la información. Estos planes no deben ser estáticos, sino que deben ser actualizados y ser sometidos a pruebas, mantenimiento y reevaluación.

Junto a la gestión de riesgos, debe aparecer la identificación de eventos que pueden causar interrupciones a los procesos comerciales, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.

**2.9.1 Business continuity and risk assessment**

o Gestión de incidentes de seguridad.

Si, el de IT se encarga de gestionarlos.

**2.9.2 Developing and implementing continuity plans including information security**

o Gestión de continuidad del negocio.

o Los auditores externos e internos de seguridad.

Auditorías financieras , de calidad por parte de los clientes , de seguridad por parte de las autoridades (secretaria de trabajo y delegación).

Falta auditoria de IT.

**2.9.3 Data protection and privacy of personal information**

o Protección de los datos y la privacidad de la información personal.

Si existen contratos de confidencialidad entre los trabajadores y los clientes.

**2.10 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE**

Debe existir una validación adecuada de los datos de entrada y de salida, controlando el procesamiento interno en las aplicaciones, y la integridad de los mensajes.

La gestión de claves debe ser tal que ofrezca soporte al uso de técnicas criptográficas en la organización, utilizando técnicas seguras.

Garantizar la seguridad de los [archivos](http://www.monografias.com/trabajos7/arch/arch.shtml) del sistema es fund,La seguridad en los procesos de desarrollo y soporte debe considerar procedimientos de control de cambios,Contar con un control de las vulnerabilidades técnicas ayudará a tratar los riesgos de una mejor manera.

amental.Deben establecerse procedimientos para el control de la instalación del software en los sistemas operacionales

o Adquisición de sistemas, desarrollo y mantenimiento.

**2.10.1 Security requirements analysis and specification**

o Criptografía.

NO

**2.10.2 Change control procedures**

o Los procedimientos de análisis de riesgos.

No hay algun documento donde se escriban los procedimientos en caso de riesgos.

**2.10.3 Control of technical vulnerabilities**

2.11 **COMPLIANCE**

Es una prioridad el buen cumplimiento de los requisitos legales para evitar las violaciones a cualquier [ley](http://www.monografias.com/trabajos4/leyes/leyes.shtml); regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad. La identificación de la legislación aplicable debe estar bien definida.

Se deben definir explícitamente, documentar y actualizar todos los requerimientos legales para cada sistema de información y para la organización en general.

o Requisitos legales esenciales o que se consideren práctica habitual de la seguridad de la información.

Si, resguarda y vigila la confidencialidad de los datos de los clientes.IFAI

**2.11.1 Intellectual property rights (IPR)**

o Derechos de la propiedad intelectual.

Si eso viene implícito en el contrato, le cede uno el derecho a la empresa de todo lo que se desarrolla dentro de ella.

**2.11.2 Protection of organizational records**

o Protección de los registros de la información.

Si,

o Relación con proveedores.

Se busca el producto que se necesite, se hace una requisición para generar la orden de compra, administración debe autorizar el gasto para esto. La orden de compra se le da al proveedor, el proveedor entrega el producto y luego te entrega una factura que se convierte en una cuenta por pagar.