1. **INTRODUCCIÓN**

En febrero del presente año, la empresa ‘Maquimetalica’ convoco a especialistas en seguridad informática de la Escuela Superior de Computo (ESCOM) con el fin de conocer sus opiniones respecto a una estrategia de seguridad informática para la empresa. De estas reuniones surgió la necesidad de que todas las áreas de la empresa cuenten con una Política de Seguridad de la Información, implementada y documentada.

En consecuencia, se conformó un grupo de trabajo con el objeto de formular un modelo de Política de Seguridad de la Información que sirviera de punto de partida para la elaboración de las políticas correspondientes en cada Organismo. Dicho grupo de trabajo decidió basar el modelo en la familia de normas ISO 27000.

El presente modelo podrá sufrir modificaciones futuras, de acuerdo a las novedades que se registren en la materia que trata, las cuales serán debidamente aprobadas y comunicadas.

* 1. **Alcance**

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del Organismo.

Debe ser conocida y cumplida por toda la planta de personal del Organismo, tanto se trate de directores o jefes de área como técnicos, y sea cual fuere su nivel jerárquico y su situación de revista.

**4 ORGANIZACIÓN DE LA SEGURIDAD**

**Generalidades**

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la empresa.

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Debe tenerse en cuenta que ciertas actividades la empresa pueden requerir que terceros accedan a información interna. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

**Objetivo**

Administrar la seguridad de la información dentro de la empresa y establecer los pasos a seguir para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Así mismo garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la empresa.

**Alcance**

Esta Política se aplicará a todas las áreas de la Empresa y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

**Responsabilidad**

Cada uno de los integrantes del equipo, que en este caso fungirán como integrantes del Comité de Seguridad de la Información serán los responsables de impulsar la implementación de la presente Política. A su vez tendrá a cargo el mantenimiento y la presentación para la aprobación de la presente Política, ante la máxima autoridad de la empresa, el seguimiento de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc.) y la proposición de asignación de funciones.

El Responsable de Seguridad Informática asistirá al personal de la empresa en materia de seguridad de la información y coordinará la interacción con Organismos especializados. Asimismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información de la empresa y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

**4.1 Infraestructura de la Seguridad de la Información**

**4.1.1 Comité de Seguridad de la Información**

La seguridad de la información es una responsabilidad del Organismo compartida por todos los directores Generales, Jefes de Área, Gerentes o equivalentes, por lo cual se crea el Comité de Seguridad de la Información, integrado por todo el personal mencionado anteriormente, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad. El mismo contará con un Coordinador, quien cumplirá la función de impulsar la implementación de la presente Política.

Este Comité tendrá entre sus funciones:

* Revisar y proponer a la máxima autoridad de la empresa para su aprobación, la Política y las funciones generales en materia de seguridad de la información.
* Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
* Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
* Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área
* Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
* Garantizar que la seguridad sea parte del proceso de planificación de la información.
* Evaluar y coordinar la implementación de controles específicos de seguridad de la  información para nuevos sistemas o servicios.
* Promover la difusión y apoyo a la seguridad de la información dentro de la empresa.
* Coordinar el proceso de administración de la continuidad de la operatoria de los  sistemas de tratamiento de la información de la empresa frente a interrupciones imprevistas.

**4.1.2 Asignación de Responsabilidades en Materia de Seguridad de la Información**

El director general asigna las funciones relativas a la Seguridad Informática de la empresa a el responsable de seguridad informática, en adelante el “Responsable de Seguridad Informática”, quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información de la empresa, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente Política.

El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación la definición y asignación de las responsabilidades que surjan del presente Modelo.

A continuación, se detallan los procesos de seguridad:

|  |
| --- |
| **Proceso** |
| Seguridad del Personal |
| Seguridad Física y Ambiental |
| Seguridad en las Comunicaciones y las Operaciones |
| Control de Accesos |
| Seguridad en el Desarrollo y Mantenimiento de Sistemas |
| Planificación de la Continuidad Operativa |

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de la información será documentada por los mismos y proporcionada al Responsable de Seguridad Informática.

**4.1.3 Proceso de Autorización para Instalaciones de Procesamiento de Información**

Los nuevos recursos de procesamiento de información serán autorizados por los responsables de las Unidades Organizativas involucradas, considerando su propósito y uso, conjuntamente con el Responsable de Seguridad Informática, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas de la empresa.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado en cada caso por el Responsable de Seguridad Informática y deberá ser autorizado por el responsable del Área Informática.

**4.1.4 Asesoramiento Especializado en Materia de Seguridad de la Información**

El Responsable de Seguridad Informática será el encargado de coordinar los conocimientos y las experiencias disponibles en el Organismo a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Con el objeto de optimizar su gestión, se habilitará al Responsable de Seguridad Informática el contacto con las Unidades Organizativas de todas las Áreas de la empresa.

**7 SEGURIDAD EN LA DEFINICIÓN DE PUESTOS DE TRABAJO Y LA ASIGNACIÓN DE RECURSOS**

**7.1 Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos**

**7.1.1 Control y Política del Personal**

Las funciones y responsabilidades en materia de seguridad serán Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que, a tal efecto, alcanzan a la empresa.

**7.1.2 Compromiso de Confidencialidad**

Como parte de sus términos y condiciones iniciales de empleo, los empleados, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la empresa. La copia firmada del Compromiso deberá ser retenida en forma segura por el Área de Recursos Humanos u otra competente.

**7.1.3 Términos y Condiciones de Empleo**

Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información.

Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades pueden extenderse más allá de los límites de la sede de la empresa y del horario normal de trabajo.

**7.2 Capacitación del Usuario**

**7.2.1 Formación y Capacitación en Materia de Seguridad de la Información**

Todos los empleados de la empresa y cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la empresa, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos que sigue la empresa.

El responsable del Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

Cada mes se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

Las siguientes áreas serán encargadas de producir el material de capacitación:

|  |
| --- |
| **Áreas Responsables del Material de Capacitación** |
| Recursos Humanos |
| Área de Informática |
| Área de Seguridad Informática |

El personal que ingrese a la empresa recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan. Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad.

**9.6 Suministros de Energía**

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

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

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

**9.7 Seguridad del Cableado**

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

1. Utilizar pisoducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información.
2. Proteger el cableado de red contra intercepción no autorizada o daño
3. Separar los cables de energía de los cables de comunicaciones para evitar  interferencias.
4. Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos  blindados.

**9.8 Mantenimiento de Equipos**

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

1. Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
2. Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
3. Eliminar la información confidencial que contenga cualquier equipamiento que sea  necesario retirar, realizándose previamente las respectivas copias de resguardo.
4. Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del responsable del Área Informática.

**9.9 Retiro de los Bienes**

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

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento.

**10.2.2 Aprobación del Sistema**

El responsable del Área Informática y el Responsable de Seguridad Informática sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva. Se deben considerar los siguientes puntos:

1. Verificar el impacto en el desempeño y los requerimientos de capacidad de las computadoras.
2. Garantizar la recuperación ante errores.
3. Preparar y poner a prueba los procedimientos operativos de rutina según normas  definidas.
4. Garantizar la implementación de un conjunto acordado de controles de seguridad.
5. Asegurar que la instalación del nuevo sistema no afectará negativamente los sistemas  existentes, especialmente en los períodos pico de procesamiento.
6. Disponer la realización de entrenamiento en la operación y/o uso de nuevos sistemas.

**10.3 Protección Contra Software Malicioso**

**10.3.1 Controles Contra Software Malicioso**

1. El Responsable de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso. El responsable del Área Informática, o el personal designado por éste, implementará dichos controles, así como desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios. Estos controles deberán considerar las siguientes acciones:
2. Prohibir el uso de software no autorizado por la empresa.
3. Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
4. Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.
5. Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles
6. Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
7. Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.

**10.5 Administración de la Red**

**10.5.1 Controles de Red**

El Responsable de Seguridad Informática definirá e implementara controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la empresa, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

* Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias.
* Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.
* Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

**10.6 Administración y Seguridad de los Medios de Almacenamiento**

**10.6.1 Procedimientos de Manejo de la Información**

Se definirán procedimientos para el manejo y almacenamiento de la información. En los procedimientos se contemplarán las siguientes acciones:

1. Incluir en la protección a documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios e instalaciones postales, uso de máquinas de fax y cualquier otro ítem potencialmente sensible.
2. Restringir el acceso solo al personal debidamente autorizado
3. Mantener un registro formal de los receptores autorizados de datos
4. Proteger los datos en espera ("colas").
5. Conservar los medios de almacenamiento en un ambiente que concuerde con las  especificaciones de los fabricantes o proveedores.

**10.6.2 Seguridad de la Documentación del Sistema**

La documentación del sistema puede contener información sensible, por lo que se considerarán los siguientes recaudos para su protección:

1. Almacenar la documentación del sistema en forma segura.
2. Restringir el acceso a la documentación del sistema al personal estrictamente  necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

**10.7 Intercambios de Información y Software**

**10.7.1 Acuerdos de Intercambio de Información y Software**

Cuando se realicen acuerdos entre empresas para el intercambio de información y software, se especificarán el grado de sensibilidad de la información de la empresa involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

1. Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
2. Procedimientos de notificación de emisión, transmisión, envío y recepción.
3. Normas técnicas para el empaquetado y la transmisión.
4. Responsabilidades y obligaciones en caso de pérdida de datos.
5. Términos y condiciones de la licencia bajo la cual se suministra el software.
6. Información sobre la propiedad de la información suministrada y las condiciones de su uso.
7. Normas técnicas para la grabación y lectura de la información y del software.
8. Controles especiales que puedan requerirse para proteger ítems sensibles.

**11.2.4 Revisión de Derechos de Acceso de Usuarios**

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate llevará a cabo un proceso formal, a intervalos regulares mensuales, a fin de revisar los derechos de acceso de los usuarios. Se deberán contemplar los siguientes controles:

1. Revisar los derechos de acceso de los usuarios a intervalos mensuales
2. Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos mensuales
3. Revisar las asignaciones de privilegios a intervalos mensuales, a fin de garantizar que no se obtengan privilegios no autorizados.

**11.3 Responsabilidades del Usuario**

**11.3.1 Equipos Desatendidos en Áreas de Usuarios**

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

Los equipos instalados en áreas de usuarios, por ejemplo, estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

El Responsable de Seguridad Informática debe coordinar con el Área de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas:

1. Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
2. Proteger las PC’s o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente.

**11.4 Control de Acceso a la Red**

**11.4.1 Política de Utilización de los Servicios de Red**

Las conexiones no seguras a los servicios de red pueden afectar a toda la empresa, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo, áreas públicas o externas que están fuera de la administración y del control de seguridad de la empresa.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

1. Identificar las redes y servicios de red a los cuales se permite el acceso.
2. Realizar normas y procedimientos de autorización para determinar las personas y las  redes y servicios de red a los cuales se les otorgará el acceso.
3. Establecer controles y procedimientos de gestión para proteger el acceso a las  conexiones y servicios de red.

**11.4.2 Autenticación de Usuarios para Conexiones Externas**

Las conexiones externas son de gran potencial para accesos no autorizados a la información de la empresa.

Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. El Responsable de Seguridad Informática, conjuntamente con el Propietario de la Información de que se trate, realizarán una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso. La autenticación de usuarios remotos puede llevarse a cabo utilizando:

1. Un método de autenticación físico (por ejemplo tokens de hardware), para lo que debe implementarse un procedimiento que incluya:
   * Asignación de la herramienta de autenticación.
   * Registro de los poseedores de autenticadores.
   * Método de revocación de acceso del autenticador, en caso de compromiso de  seguridad.
2. Un protocolo de autenticación (por ejemplo desafío / respuesta), para lo que debe implementarse un procedimiento que incluya:
   * Establecimiento de las reglas con el usuario.
   * Establecimiento de un ciclo de vida de las reglas para su renovación.

Los procedimientos y controles de re-llamada, o dial-back, pueden brindar protección contra conexiones no autorizadas a las instalaciones de procesamiento de información de la empresa.

**11.4.8 Seguridad de los Servicios de Red**

El Responsable de Seguridad Informática junto con el responsable del Área Informática definirán las pautas para garantizar la seguridad de los servicios de red de la empresa, tanto públicos como privados. Para ello se tendrán en cuenta las siguientes directivas:

1. Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
2. Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
3. Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran  presentar.
4. Instalar periódicamente las actualizaciones de seguridad.

Dicha configuración será revisada periódicamente por el responsable de Seguridad Informática.

**13.2.1 Control del Software Operativo**

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas:

* Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.
* Toda aplicación tendrá un único responsable designado formalmente por el responsable del Área Informática.
* El responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de “implementador” al personal de su área que considere adecuado, quien tendrá como funciones principales:

1. Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
2. Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
3. Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.
4. Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

1. Guardar sólo los ejecutables en el ambiente de producción.
2. Retener las versiones previas del sistema, como medida de contingencia.
3. Definir un procedimiento que establezca los pasos a seguir para implementar las  autorizaciones y conformes pertinentes, las pruebas previas a realizarse, etc.
4. Evitar, que la función de implementador sea ejercida por personal que pertenezca al  sector de desarrollo o mantenimiento.

**14.3 Firma Digital**

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Pueden aplicarse a cualquier tipo de documento que se procese electrónicamente. Se implementan mediante el uso de una técnica criptográfica sobre la base de dos claves relacionadas de manera única, donde una clave, denominada privada, se utiliza para crear una firma y la otra, denominada pública, para verificarla.

Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

Se recomienda que las claves criptográficas utilizadas para firmar digitalmente no sean empleadas en procedimientos de cifrado de información. Dichas claves deben ser resguardadas bajo el control exclusivo de su titular.

En algunos casos podría ser necesario establecer acuerdos especiales para respaldar el uso de las firmas digitales. A tal fin se deberá obtener asesoramiento legal con respecto al marco normativo aplicable y la modalidad del acuerdo a implementar.

**14.3.1 Normas Procedimientos y Métodos**

Se redactarán las normas y procedimientos necesarios para:

1. Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
2. Generar y obtener certificados de clave pública de manera segura.
3. Distribuir claves de forma segura a los usuarios que corresponda, incluyendo  información sobre cómo deben activarse cuando se reciban.
4. Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los  usuarios autorizados.
5. Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse  las claves.
6. Recuperar claves pérdidas o alteradas como parte de la administración de la continuidad de las actividades de la empresa, por ejemplo para la recuperación de la información cifrada.
7. Archivar claves, por ejemplo, para la información archivada o resguardada.
8. Destruir claves.

**15 CUMPLIMIENTO**

**Generalidades**

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deben estar debidamente definidos y documentados.

El Área Legal de la empresa, será responsable de encuadrar jurídicamente la formulación e implementación de la política.

**Objetivos**

Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la empresa y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.

Determinar los plazos para el mantenimiento de información y para la recolección de evidencia de la empresa.

**Alcance**

Esta Política se aplica a todo el personal de la empresa, cualquiera sea su situación de revista.

Asimismo, se aplica a los sistemas de información, normas, procedimientos, documentación y plataformas técnicas de la empresa y a las auditorías efectuadas sobre los mismos.

**Responsabilidad**

El Responsable de Seguridad Informática cumplirá las siguientes funciones:

1. Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la  conservación de registros.
2. Realizar revisiones periódicas de todas las áreas de la empresa a efectos de  garantizar el cumplimiento de la política, normas y procedimientos de seguridad.
3. Verificar periódicamente que los sistemas de información cumplan la política, normas y  procedimientos de seguridad establecidos.
4. Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones  de auditoría.

Todos los empleados de los mandos medios y superiores conocerán, comprenderán, darán a conocer, cumplirán y harán cumplir la presente Política y la normativa vigente.

**15.1 Cumplimiento de Requisitos Legales**

**15.1.1 Identificación de la Legislación Aplicable**

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

**15.1.2 Derechos de Propiedad Intelectual**

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

Los empleados únicamente podrán utilizar material autorizado por la empresa.

La empresa solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordados y lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.