## 4 ORGANIZACIÓN DE LA SEGURIDAD

### 4.1 Infraestructura de la Seguridad de la Información

### 4.1.1 Comité de Seguridad de la Información

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

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.

Al final de cada año se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas de la empresa, salvo que se presente algún fallo antes de cumplirse dicho tiempo, en ese caso, se verificara en ese momento para descartar una posible falla por compatibilidad.

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

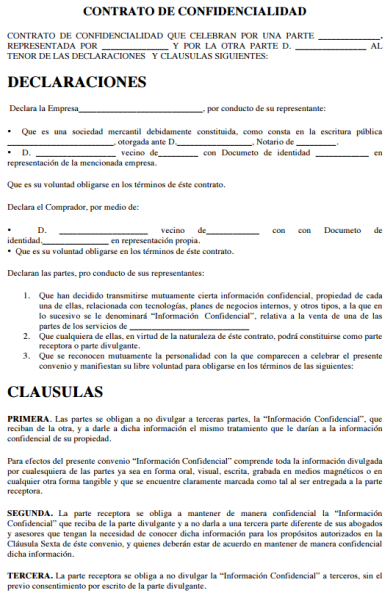
El Responsable de Seguridad Informática será el encargado de coordinar los conocimientos y las experiencias disponibles en el Organismo a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Con el objeto de optimizar su gestión, se habilitará al Responsable de Seguridad Informática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

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.



**CONTRATO DE CONFIDENCIALIDAD**

CONTRATO DE CONFIDENCIALIDAD QUE CELEBRAN POR UNA PARTE _____, REPRESENTADA POR _____ Y POR LA OTRA PARTE D. _____ AL TENOR DE LAS DECLARACIONES Y CLAUSULAS SIGUIENTES:

**DECLARACIONES**

Declara la Empresa_____, por conducto de su representante:

- Que es una sociedad mercantil debidamente constituida, como consta en la escritura pública _____, otorgada ante D._____ Notario de _____.
- D. _____ vecino de_____ con Documeto de identidad _____ en representación de la mencionada empresa.

Que es su voluntad obligarse en los términos de éste contrato.

Declara el Comprador, por medio de:

- D. _____ vecino de_____ con con Documeto de identidad_____ en representación propia.
- Que es su voluntad obligarse en los términos de éste contrato.

Declaran las partes, pro conducto de sus representantes:

1. Que han decidido transmitirse mutuamente cierta información confidencial, propiedad de cada una de ellas, relacionada con tecnologías, planes de negocios internos, y otros tipos, a la que en lo sucesivo se le denominará "Información Confidencial", relativa a la venta de una de las partes de los servicios de _____.
2. Que cualquiera de ellas, en virtud de la naturaleza de éste contrato, podrá constituirse como parte receptora o parte divulgante.
3. Que se reconocen mutuamente la personalidad con la que comparecen a celebrar el presente convenio y manifiestan su libre voluntad para obligarse en los términos de las siguientes:

**CLAUSULAS**

**PRIMERA**. Las partes se obligan a no divulgar a terceras partes, la "Información Confidencial", que reciban de la otra, y a darle a dicha información el mismo tratamiento que le darían a la información confidencial de su propiedad.

Para efectos del presente convenio "Información Confidencial" comprende toda la información divulgada por cualesquiera de las partes ya sea en forma oral, visual, escrita, grabada en medios magnéticos o en cualquier otra forma tangible y que se encuentre claramente marcada como tal al ser entregada a la parte receptora.

**SEGUNDA.** La parte receptora se obliga a mantener de manera confidencial la "Información Confidencial" que reciba de la parte divulgante y a no darla a una tercera parte diferente de sus abogados y asesores que tengan la necesidad de conocer dicha información para los propósitos autorizados en la Cláusula Sexta de éste convenio, y quienes deberán estar de acuerdo en mantener de manera confidencial dicha información.

**TERCERA.** La parte receptora se obliga a no divulgar la "Información Confidencial" a terceros, sin el previo consentimiento por escrito de la parte divulgante.

### 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.

*<- Formato del contrato de confidencialidad*

### 7.1.3 Términos y Condiciones de Empleo

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 |

### 9.6 Suministros de Energía

Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
b) 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.
c) 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.

### 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:

a) Utilizar pisoducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información.
b) Proteger el cableado de red contra intercepción no autorizada o daño
c) Separar los cables de energía de los cables de comunicaciones para evitar interferencias.

d) 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:

a) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
b) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
c) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.
d) 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.

### 10.3 Protección Contra Software Malicioso

### 10.3.1 Controles Contra Software Malicioso

a) 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:

b) Prohibir el uso de software no autorizado por la empresa.

c) 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.

d) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.

e) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles

f) 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.

g) 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:

a. 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.
b. Restringir el acceso solo al personal debidamente autorizado
c. Mantener un registro formal de los receptores autorizados de datos
d. Proteger los datos en espera ("colas").
e. 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:

a) Almacenar la documentación del sistema en forma segura.

b) 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

### 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:

a. Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
b. Procedimientos de notificación de emisión, transmisión, envío y recepción.
c. Normas técnicas para el empaquetado y la transmisión.
d. Responsabilidades y obligaciones en caso de pérdida de datos.
e. Términos y condiciones de la licencia bajo la cual se suministra el software.
f. Información sobre la propiedad de la información suministrada y las condiciones de su uso.
g. Normas técnicas para la grabación y lectura de la información y del software.
h. Controles especiales que puedan requerirse para proteger ítems sensibles.

.

### 11.3 Responsabilidades del Usuario

### 11.3.1 Equipos Desatendidos en Áreas de Usuarios

Los usuarios cumplirán con las siguientes pautas:

a) 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.

b) 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

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

a) Identificar las redes y servicios de red a los cuales se permite el acceso.
b) 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.
c) 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

La autenticación de usuarios remotos puede llevarse a cabo utilizando:

a) 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.

b) 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.

### 11.4.7 Seguridad de los Servicios de Red

Se tendrán en cuenta las siguientes opciones:

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

### 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:
- Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
- 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.
- 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.
- Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.
- Otros controles a realizar son:
- Guardar sólo los ejecutables en el ambiente de producción.
- Retener las versiones previas del sistema, como medida de contingencia.
- Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformes pertinentes, las pruebas previas a realizarse, etc.
- Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

### 14.4 Normas Procedimientos y Métodos

Se redactarán las normas y procedimientos necesarios para:

a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
b) Generar y obtener certificados de clave pública de manera segura.
c) Distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.
d) Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.
e) Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.
f) 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.
g) Archivar claves, por ejemplo, para la información archivada o resguardada.
h) Destruir claves.

## 16 CUMPLIMIENTO

### 16.1 Cumplimiento de Requisitos Legales

#### 16.1.1 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.

#### 16.1.2 Derechos 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 acordadas y lo dispuesto por la normativa vigente.

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