### Sistemas de Soporte S. A.

**Políticas de Seguridad de la Información**

**José Videla Quezada**

Responsable

# 1. INTRODUCCION

El objetivo de este documento es establecer las políticas de seguridad de la información para **Sistemas de Soporte S. A.**, proteger los recursos de informáticos valiosos de la institución, tales como la información, el hardware o el software. A través de la adopción de las medidas adecuadas, la política de seguridad informática ayuda a la organización a cumplir sus objetivos, protegiendo sus recursos financieros, sus sistemas, su reputación, su situación legal, y otros bienes tanto tangibles como inmateriales.

Esta política está enfocada para cada uno de los miembros de la institución y debe concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la institución.

Este documento es una guía de políticas y procedimientos relacionadas con la infraestructura tecnológica de **Sistemas de Soporte S. A**. en cuanto a los políticas de seguridad de la información. Desarrollar una política de seguridad informática significa planear, organizar, dirigir y controlar las actividades tecnológicas para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la institución.

# 2. JUSTIFICACION

La seguridad informática aplica técnicas fundamentadas para preservar la información y los diferentes recursos informáticos con que cuenta **Sistemas de Soporte S. A**. La política de seguridad informática es el conjunto de normas, reglas, procedimientos y prácticas que regulan la protección de la información contra la pérdida de forma accidental como intencionada.

# 3. OBJETIVOS

Establecer la política de Seguridad Informática que apoye la Seguridad de la Información, entendida como la preservación de la integridad, confidencialidad y disponibilidad, así como instrumentar y coordinar acciones para minimizar daños a la infraestructura tecnológica y a los sistemas informáticos. El objetivo principal de la Seguridad Informática será proteger desde el ámbito tecnológico la información electrónica institucional, los recursos informáticos y los servicios tecnológicos necesarios para que **Sistemas de Soporte S. A** pueda cumplir con su misión.

# 

# 4. ALCANCE

# 

Se definen políticas y lineamientos con el propósito de cumplir con los objetivos de la institución en seguridad informática; y para ello se establecen:

* **Políticas de seguridad:** Para definir controles que proporcionan directivas y consejos de gestión para mejorar la seguridad de los activos de información.
* **Políticas Administrativas u Organizarles:** Que define controles para facilitar la gestión de la información en **Sistemas de Soporte S. A**.
* **Políticas para Gestión de Activos:** Que establece controles para catalogar los activos y protegerlos eficazmente.
* **Políticas de Seguridad para Personas:** Que permite establecer controles para reducir los riesgos de error humano, robo, fraude y utilización abusiva de los equipamientos.
* **Políticas de Seguridad Física**. Establece controles para impedir la violación, deterioro y la perturbación de las instalaciones y datos.
* **Políticas de Gestión de las Operaciones:** Define controles para garantizar un funcionamiento seguro y adecuado de los dispositivos de tratamiento de la información.
* **Políticas de Control de Acceso a los Datos:** Identificar medios para impedir accesos no autorizados y registro de los accesos efectuados**.**
* **Políticas para Adquisición, Desarrollo y Mantenimiento de Software:** Controles para establecer racionalización de gastos, aspectos a tener en cuenta al momento de adquisiciones y establecimiento de estándares.
* **Políticas para Gestión de Incidentes:** Clasificación de los incidentes según el grado en que afecten el normal funcionamiento del negocio. Controles para gestionar las incidencias que afectan a la seguridad de la Información.
* **Políticas para la Continuidad de la Operación:** Controles para reducir los efectos de las interrupciones de actividad y proteger los procesos esenciales de **Sistemas de Soporte S. A** contra averías y siniestros mayores.

|  |
| --- |
| POLITICAS DE SEGURIDAD |
| **1** **Responsables** |
| **1.1 Responsable de** **Seguridad Informática** |
| **Objetivos:** Es quien cumplirá funciones relativas a la seguridad de los sistemas de información, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente política. |

|  |
| --- |
| **1.2 Propietarios de la Información** |
| **Objetivos:** deben clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia. |

|  |
| --- |
| **1.3 Responsables por Área** |
| **Objetivos:** cumplirá la tarea de notificar a todo el personal respecto del cumplimiento de la política de seguridad de la Información y de todos los alcances de esta. Asimismo, tendrá a su cargo la notificación de la presente política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los compromisos de confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad. |

|  |
| --- |
| **1.4 Usuarios de la información** |
| **Objetivos:** Los  **Usuarios de la información** y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente. |

|  |
| --- |
| **2**  **Ingreso y salida de equipos** |
| **2. 1 Ingreso de Equipos** |
| **Objetivos:** Los equipos externos que ingresen a la **Sistemas de Soporte S. A** deben ser registrados por el número de serial que lo identifica, marca, propietario y hora de ingreso. |

|  |
| --- |
| **2. 2 Egreso de Equipos** |
| **Objetivos:** Para los equipos que salgan de **Sistemas de Soporte S. A** se debe verificar en la planilla el registro de ingreso confrontando el número de serial, marca y fecha y complementar esta información con la hora de salida y la firma de quien sale con dicho equipo. |

|  |
| --- |
| **2. 3 Otros casos** |
| **Objetivos:** En caso que el equipo saliente sea de propiedad de Sistemas de Soporte S. A debe tener autorización expresa por el encargado de área. |

|  |
| --- |
| 3 Políticas |
| **3.1 Políticas Administrativas u Organizacionales** |
| **Objetivos:** Controles para facilitar la gestión de la información en **Sistemas de Soporte S. A**, garantizando que existan responsabilidades claramente asignadas en todos los niveles de **Sistemas de Soporte S. A.** Todos los empleados y particulares que tengan acceso a los activos de información de **Sistemas de Soporte S. A**, tendrán el compromiso de cumplir las políticas, normas y procedimientos que se dicten en esta materia, así como reportar los incidentes que detecten. |

|  |
| --- |
| **3.2 Políticas para gestión de Activos** |
| **Objetivos:** **Objetivos:** Controles para catalogar los activos y protegerlos eficazmente. Toda la información sensible, así como los activos donde ésta se almacena o procesa, deben ser inventariados, asignarles un responsable y clasificarlos de acuerdo con los requerimientos en materia de seguridad de la información. A partir de esta clasificación se deben establecer los niveles de protección orientados a determinar, a quién se le permite el manejo de la información, el nivel de acceso a la misma y los procedimientos para su manipulación. La clasificación debe revisarse periódicamente y atender a los cambios que se presenten en la información o la estructura que puedan afectarla. |

## 

## 

|  |
| --- |
| 4. Inventario |
| **4.1 Inventario de activos** |
| **Objetivos:** Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información. El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad semestral.  El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa. |

## 

|  |
| --- |
| **4.2 Clasificación de la información** |
| **Objetivos:** Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad. Se establece el criterio de clasificación de la información en función a estas características: |
| **4.2.1 Confidencialidad:**  Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la Institución o no. Tipo: PUBLICO   1. Información que puede ser conocida y utilizada por todos los empleados de la Institución y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la Institución o terceros. Tipo: RESERVADA – USO INTERNO 2. Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la Institución o a terceros. Tipo: RESERVADA - CONFIDENCIAL 3. Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la Institución, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros. Tipo: RESERVADA SECRETA |
| **4.2.2 Integridad:**   1. Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria de la Institución. 2. Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para la Institución o terceros. 3. Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la Institución o terceros. 4. Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a la institución o a terceros. |
| **4.2.3 Disponibilidad:**   1. Información cuya inaccesibilidad no afecta la operatoria de la Institución. 2. Información cuya inaccesibilidad permanente durante a una semana podría ocasionar pérdidas significativas para la Institución, el Sector Público Nacional o terceros. 3. Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la Institución, al Sector Público Nacional o a terceros. 4. Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas a la Institución, al Sector Público Nacional o a terceros.   Al referirse a pérdidas, se contemplan aquellas mesurables (materiales) y no mesurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).  Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:   * + CRITICIDAD BAJA: Ninguno de los valores asignados superan el 1.   + CRITICIDAD MEDIA: Alguno de los valores asignados es 2   + CRITICIDAD ALTA: alguno de los valores asignados es 3   Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:   * + Asignarle una fecha de efectividad.   + Comunicárselo al depositario del recurso.   + Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.   Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deberán tener acceso a la misma. |

## 

|  |
| --- |
| 5. Seguridad |
| **5.1 Seguridad para Personas** |
| **Objetivos:** Controles para reducir los riesgos de error humano, robo, fraude y utilización abusiva de los equipamientos. Se deben tener controles que permitan verificar la idoneidad e identidad, ética profesional y conducta. Se debe firmar un acuerdo de confidencialidad que se hace extensivo a los contratistas y terceros que tengan acceso a la información.  Deben existir mecanismos de información y capacitación para los usuarios en materia de seguridad, así como de reporte de incidentes que puedan afectarla. Los empleados deben cooperar con los esfuerzos por proteger la información, así como consultar con el encargado de la seguridad de la información, en caso de duda o desconocimiento de un procedimiento formal, ya que esto no lo exonera de una acción disciplinaria que deba llevarse a cabo cuando se incurra en violaciones a las políticas o normas de seguridad.   * Al momento de asignar un equipo informático a un usuario, este debe hacerse responsable de el mismo y comprometerse a reportar cualquier falla y entregarlo en perfecto estado. * Los propietarios de la información deben definir los niveles de acceso de cada usuario. * Los nuevos empleados deben firmar un acuerdo de confidencialidad * Se deben realizar capacitaciones periódicas sobre los sistemas de información y el uso de la misma y de acspectos de seguridad de informática * Los usuarios de servicios de información, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Responsable de Seguridad Informática. |

|  |
| --- |
| 5.1 . Seguridad para Equipos |
| **Objetivos:** Controles para impedir la violación, deterioro y la perturbación de las instalaciones y datos. Establecerse áreas seguras para el, almacenamiento y procesamiento de información; éstas deben contar con protecciones físicas y ambientales acordes a los activos que protegen. Esta seguridad debe mantenerse en los momentos de mantenimiento, cuando la información o los equipos que la contienen deben salir de la Institución o cuando se deben eliminar o dar de baja, para lo cual deben existir procedimientos especiales.   * Los equipos deben ser apagados todos los días, exceptuando los servidores * Se deben definir áreas seguras para el alojamiento físico de servidores |
| 5.1.1 Controles de Acceso Físico Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad Informática, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, las siguientes características:   * Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia. * Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se mantendrá un registro protegido para permitir auditar todos los accesos. |

|  |
| --- |
| 6. Seguridad Equipamientos |
| **6.1 Servidores** |
| **Objetivos:** Físicos y Virtuales de diferentes especificaciones técnicas. Homologados con los mejores fabricantes y configurados es esquemas de alta disponibilidad y desempeño. |
| **6.2 Software:** |
| **Objetivos:** Licenciamiento acorde a los requerimientos de la solución. Incluyendo soporte y actualizaciones con sus fabricantes, distribuidores o agentes autorizados. Licenciamiento Microsoft por consumo. |
| **6.3 Conectividad:** |
| **Objetivos:** Servicios de conexión Internet, MPLS o de datos desde las sedes de nuestros clientes a nivel local o regional hasta nuestros data center. Diferentes opciones de configuración LAN, según disponibilidad y tráfico dimensionado. Configuraciones dedicadas a las redes de gestión y monitoreo. |
| **6.4 Seguridad:** |
| **Objetivos:** Servicios de Firewall e IPS (protección contra intrusos) para sus perímetros de conectividad, para sus capas lógicas. VPN´s SSL e IPSec, Antivirus. |
| **6.5 Almacenamiento:** |
| **Objetivos:** A través de opciones de plataformas con discos FC, SAS y SATA. |
| **6.6 Backup y continuidad:** |
| **Objetivos:** Soluciones y políticas de backup para el almacenamiento local o externo de servidores ubicados en nuestros data center. Opciones de replicación de almacenamiento entre nuestros data center. Toma y respaldo de imágenes de servidores físicos y virtuales. |
| **6.7 Servicios de red:** |
| **Objetivos:** Balanceo de carga para servidores y/o aplicaciones a nivel local o global, NTP, DNS, Relay de Correo, Replicación de servidores, sistemas operativos, aplicaciones. |
| **6.7 Servicios:** |
| **Objetivos:** Administración y operación de plataformas de hardware, aplicaciones, gestión y monitoreo. Control y gestión de cambios, eventos e incidentes. Monitoreo avanzado, Reporting, Análisis de vulnerabilidad y remediación. |

|  |
| --- |
| **6.8 Ubicación y Protección del Equipamiento y Copias de Seguridad** |
| **Objetivos:** El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:  Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.   * Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.   Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida. Y adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por: robo o hurto, incendio, explosivos, humo, inundaciones o filtraciones de agua (o falta de suministro), polvo, vibraciones, efectos químicos, interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión), radiación electromagnética, derrumbes |
| **6.9 Mantenimiento de Equipos** |
| **Objetivos:** Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:   * Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal de la Dirección de Tecnologías y Apoyo. La dirección mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo. * Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento. * Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado. * Registrar el retiro de equipamiento de las instalaciones para su mantenimiento. * Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo. |

## 

|  |
| --- |
| **6.10 Políticas de Escritorios y Pantallas Limpias.** |
| **Objetivos:** Se adopta una política de escritorios limpios para proteger documentos en papel y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.  Se aplicarán los siguientes lineamientos:   * Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo. * Guardar bajo llave la información sensible o crítica de la Institución (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina. * Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción. |

## 

|  |
| --- |
| **6.10** Retiro de los Bienes |
| El equipamiento, la información y el software no serán retirados sin autorización formal. Periódicamente, se llevarán a cabo comprobaciones para detectar el retiro no autorizado de activos. El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones. |

## 

|  |
| --- |
| 7 Procedimientos de Manejo de Incidentes |
| **7.1 Reporte de incidentes:** |
| **Objetivos:** Todos los incidentes relacionados con la seguridad de la información tendrán que ser reportados mediante el centro de soporte, el cual informará al área encargada de la seguridad de la información esto, siempre y cuando se presenten indicios que involucren la seguridad de la información. |
| **7.2 Clasificación de incidentes:** |
| **Objetivos:** Según sea el caso se clasificaran los incidentes dentro de las siguientes categorías:   * + Acceso no autorizado   + Modificación de recursos no autorizado (Plagios, Base de datos)   + Uso inapropiado de recursos (Divulgación)   + No disponibilidad (Denegación de Servicio)   + Otros |
| **7.3 Tratamiento de incidentes:** |
| **Objetivos:** Los miembros del departamento de TI se encargaran de la recepción y gestión de los incidentes, también informaran los avances y hallazgos encontrados a los diferentes clientes y darán cumplimento a la política de tratamiento de incidentes.  **Cliente interno y externo**.     * + Los clientes internos y externos tendrán la responsabilidad de reportar los incidentes mediante los medios de comunicación dispuestos para este fin |

.

## 

|  |
| --- |
| 8 Reglas de Control de Acceso |
| **8.1 Registro de Usuarios** |
| **Objetivos:** El Responsable de Seguridad Informática definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, el cual debe comprender:   * Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. * Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad de la Institución. * Entregar a los usuarios un detalle escrito de sus derechos de acceso. * Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso. * Mantener un registro formal de todas las personas registradas para utilizar el servicio. * Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la Institución o sufrieron la pérdida/robo de sus credenciales de acceso. * Efectuar revisiones periódicas con el objeto de cancelar identificadores y cuentas de usuario redundante, inhabilitar cuentas inactivas por más de 30 días. * Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal intenta accesos no autorizados. |
| **8.2 Administración de Privilegios** |
| **Objetivos:** Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente. |