

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

COORDINACION ADMINISTRATIVA DE SISTEMAS

ESE ANTONIO NARIÑO EN LIQUIDACIÓN

ENERO 2009

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la ESE Antonio Nariño en liquidación busca evitar que las amenazas latentes en el entorno, puedan acceder, manipular o deteriorar la información producida por los procesos de la organización y disminuir la posible pérdida de información.

1. ACCESO A LA INFORMACION
2. USO DE CONTRASEÑAS
3. HARDWARE Y SOFTWARE
4. VIRUS
5. COPIAS DE SEGURIDAD

1. ACCESO A LA INFORMACION

La divulgación de información generada en la ESE Antonio Nariño en liquidación está supeditada al estudio y aprobación por parte del Apoderado.

No deberá existir sobre el escritorio información confidencial o de importancia para la organización a la vista de cualquier persona, ni referencias sobre los códigos de acceso de la persona encargada de algún cargo que sea parte de la organización.

Se restringe el acceso a las áreas de sistemas, archivos Administrativos, archivo clínico, tesorería y nómina, al personal no autorizado con el fin de salvaguardar la información que allí se almacena.

Las puertas de acceso a dichas dependencias deben permanecer cerradas.

Cuando las personas con permisos se encuentren en las respectivas dependencias de la institución, estarán en todo momento, acompañadas del personal de la ESE Antonio Nariño en liquidación

La Coordinación Administrativa y de Sistemas restringe el acceso a las bases de datos en las que se almacena la información institucional, para asegurar su correcta utilización.

La oficina de Archivo se responsabiliza de toda la documentación que ingrese a la entidad a través de ella, prohibiendo el recibo de documentos en otras áreas.

Para dar cumplimiento a esta política, la institución diseña protocolos y procedimientos que regulan la administración de la información.

Las solicitudes de información para presentación de informes, debe contener todas las especificaciones necesarias de acuerdo con el informe requerido y deben ser justificadas y autorizadas por el jefe del área solicitante.

2. USO DE CONTRASEÑAS

- Todos los funcionarios que deban tener acceso a las herramientas que apoyan el sistema de información, cuentan con clave de acceso y tiene definidos perfiles de usuarios que aseguren la autorización para grabar, modificar y consultar información.
- Las claves asignadas para acceder a los sistemas de información son de uso personal e intransferible y está bajo la responsabilidad de cada usuario
- Los funcionarios deben cambiar la clave cuando lo considere necesario debido a alguna vulnerabilidad en los criterios de seguridad.
- Cuando el funcionario deja el puesto de trabajo, se deben cerrar las aplicaciones que se estén utilizando.
- Los archivos administrativos que se utilizan en procesos institucionales o equipos de cómputo requieren una clave o contraseña especial, esta debe ser notificada a la Coordinación Administrativa y de Sistemas.

3. HARDWARE Y SOFTWARE

- No se pueden ingresar a la ESE Antonio Nariño en Liquidación hardware ni software personales sin previa autorización de la Coordinación Administrativa y de Sistemas.
- No se deben bajar ni actualizar programas desde Internet en los equipos de la ESE Antonio Nariño en Liquidación, salvo las actualizaciones configuradas por la coordinación de sistemas.
- La instalación de software que desde el punto de vista de la Coordinación Administrativa y de sistemas pudiera poner en riesgo los recursos de la institución no está permitida.

4. VIRUS

- Los Usuarios de cada uno de los Sistemas de información son responsables de solicitar soporte informático en caso de encontrar situaciones sospechosas en el sistema.
- Para la utilización de medios magnéticos propios se debe realizar previamente el proceso de vacunación.
- No instalar "vacunas" sin la autorización de la Coordinación de Sistemas. Estas aunque parezca paradójico, pueden estar infectadas.

5. COPIAS DE SEGURIDAD

En un momento en el que la seguridad es la clave de la supervivencia de los negocios, arbitrar una política proactiva se ha convertido en un imperativo. Algo fundamental para devolver la operatividad plena a una organización en caso de tener que poner en marcha el plan de contingencia que permita la recuperación y la continuidad del proceso. Para los procesos críticos se deberá destinar la máxima atención y recursos, con centros o equipos de respaldo.

- Los responsables del manejo de cada uno de los sistemas deben realizar copias de seguridad diarias de las actividades ó transacciones realizadas en los discos duros asignados por la Coordinación de Sistemas.
- Los Líderes de los procesos deben velar porque los procesos de información que se realizan en sus áreas estén soportados por un proceso de respaldo de la información y por lo tanto deben solicitar a la Coordinación Administrativa y de Sistemas para que se diseñe el mecanismo de respaldo que asegure la información.
- El control y supervisión del proceso de respaldo de la información debe ser del líder del área, donde se genera la información.
- La Coordinación Administrativa y de Sistemas debe elaborar un plan de copias de seguridad de la información.
- La Coordinación de Sistemas debe crear mecanismos que garanticen su correcto almacenamiento.
- Para los aplicativos críticos, se debe realizar un respaldo diariamente en el equipo donde se tiene el aplicativo y uno semanal que será enviado a la Coordinación Administrativa y de Sistemas (Proveedor del Sistema de Información).
- Se verificara por parte de La Coordinación de Sistemas la realización de los respectivos respaldos en cada uno de los puestos de trabajo, el incumplimiento de dicha norma será notificado a la respectiva Gerencia del proceso liquidatorio.

Los mecanismos de respaldo de aplicativos críticos son los siguientes:

Diario:

Se guarda backup diario de lunes a viernes en el disco duro del equipo donde estén los aplicativos críticos, utilizando los scripts implementados por la Coordinación de Sistemas.

Semanal:

Este debe almacenar la información correspondiente a los movimientos realizados todos días de la semana, utilizando los scripts implementados por la Coordinación de

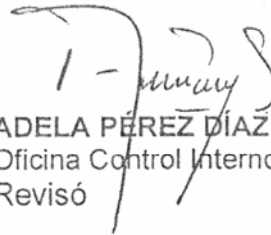
Sistemas, debe realizarse los días viernes, se debe guardar el respaldo en el disco duro de una de las maquinas de la red y debe ser enviada a la oficina de sistemas de la ESE Antonio Nariño en Liquidación.



REYNEL FERNANDO BEDOYA RODRIGUEZ
Apoderado General Liquidador
Aprobó y Autorizó



JULIO CESAR SUÁREZ ALVAREZ
Coordinador Administrativo y de Sistemas
Elaboró



ADELA PÉREZ DÍAZ
Oficina Control Interno de Gestión
Revisó