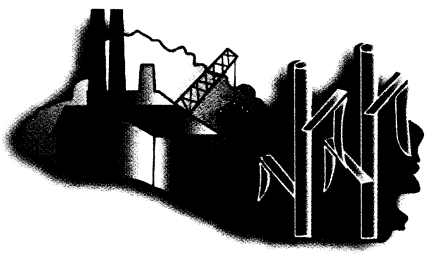
Consejo Salvadoreño de la Agroindustria Azucarera



CONSAA

Manual de Sistemas Informáticos

INDICE

INTRODUCCION

Actualmente las instituciones públicas utilizan las "Tecnologías de la Información" como una herramienta que apoya el logro de los objetivos institucionales de una forma cada vez más estratégica y eficiente. Se define Tecnología de la Información (TI), a las herramientas y métodos utilizados para recabar, retener o distribuir información, la cual se encuentra por lo general, relacionada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones.

En ese sentido, se plantea y se presenta el Manual de Sistemas Informáticos del Consejo Salvadoreño de la Agroindustria Azucarera (CONSAA), el cual representa una importante herramienta que servirá para garantizar razonablemente el uso de los equipos informáticos, la confiabilidad de los registros, contribuir con su eficiencia y garantizar la calidad en la gestión.

OBJETIVO GENERAL

Definir políticas que simplifiquen la ejecución y control de las actividades tecnológicas en las diferentes unidades organizativas de la institución.

OBJETIVOS ESPECÍFICOS

- Crear Políticas de los sistemas de información del Consejo para fortalecer el Control Interno.
- Definir responsabilidades en el uso de los sistemas informáticos.
- Establecer las diferentes restricciones y prohibiciones al utilizar los sistemas informáticos.

MARCO LEGAL

Normas Técnicas de Control Interno Especificas del Consejo Salvadoreño de la Agroindustria Azucarera.

POLITICAS GENERALES

1. Todo usuario con acceso a un sistema de información dispondrá de una autorización de acceso, personal e intransferible, compuesta al menos de identificador de usuario y contraseña.

2. Las contraseñas tendrán plazo de vigencia, que en ningún caso podrá ser superior a los 6 meses.

3. Cada sistema informático deberá tener segmentados por roles a sus usuarios que permitan los cambios o modificaciones necesarias autorizadas.

4. Si los usuarios sospechan que su acceso autorizado (identificador de usuario y/o contraseña) está siendo utilizado por otra persona, deberá proceder a informar y solicitar una nueva contraseña.

5. Ningún usuario deberá utilizar credenciales de acceso de otros usuarios, aunque dispongan de la autorización del propietario, salvo a la autorización dada por la Dirección Ejecutiva o jefe inmediato.

6. En caso de traslado o cese del usuario del sistema, el jefe de la unidad deberá informar a la Unidad Administrativa para realizar la baja a las credenciales asignadas.

7. Las contraseñas para los accesos a sistemas informáticos deben poseer una longitud mínima de seis caracteres y que sean difíciles de descifrar por otros usuarios.

8. Independientemente de las circunstancias, las contraseñas individuales de las cuentas de correo o de usuario de la red, no deberán compartirse o divulgarse a terceros sin la debida autorización de la Dirección Ejecutiva o Jefe de la Unidad respectiva; efectuarlo supone responsabilidad por las acciones de terceros al usuario autorizado.

9. Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

10. Los nombres de usuarios deberán estar formados por identificadores de sus nombres y/o apellidos, con el fin de evitar duplicidades y definir responsabilidades en el registro de información.

11. Los usuarios deben notificar a su jefatura inmediata cualquier incidencia detectada que afecte o pueda afectar la seguridad de los datos, tales como: pérdida de archivos en los discos duros de sus equipos o memorias USB, sospechas de uso indebido de sus equipos o accesos no autorizados por otras personas.

12. Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona, ni mantenerla por escrito a la vista, ni al alcance de terceros. Si un usuario tiene sospechas que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefatura inmediata y éste reportar al responsable de la administración de la red.

13. Deben identificarse las responsabilidades en los procedimientos de las Unidades de Gestión por la asignación de roles de trabajo y sus autorizaciones respectivas.

Capítulo I: Servicios contratados por el Consejo

1. Para la realización de las actividades de carácter informático, el CONSAA podrá contratar diferentes servicios relacionados a las tecnologías de la información, tomando como base los servicios siguientes:

    a. Prestación de servicios de enlace de Internet.
    b. Prestación de servicios de conectividad para transmisión de datos entre el Ministerio de Hacienda y el CONSAA.
    c. Prestación de servicios de Alquiler de equipos de Access Point, incluyendo un switch.
    d. Prestación de servicios de Mantenimiento Preventivo, Correctivo y Soporte Técnico para equipo informático propiedad del CONSAA.
    e. Prestación de servicios de alojamiento de web hosting.
    f. Servicios de creación, mantenimiento y soporte técnico de sistemas informáticos.
    g. Otros servicios necesarios para el buen funcionamiento informático de los equipos de la Institución.

2. Todas las especificaciones técnicas relacionadas a estos servicios, serán establecidas en los contratos celebrados entre el Consejo y las personas naturales o jurídicas contratadas.

Capítulo II: Adquisición de Equipo Informático

1. Cuando se requiera la compra de equipo informático: computadoras, CPU, escáneres, UPS e impresores, la unidad solicitante deberá requerir a la persona natural o jurídica que esté prestando los servicios de mantenimiento preventivo, correctivo y soporte técnico del equipo informático del Consejo, una recomendación de las especificaciones y características técnicas mínimas necesarias que debe cumplir el bien solicitado y de acuerdo a la naturaleza de las funciones que desempeñe el solicitante; a efecto de que el equipo a adquirir sea compatible y eficiente para las labores a desempeñar.

2. Si al momento de solicitarse el equipo antes detallado, no se cuenta con los servicios de mantenimiento preventivo, correctivo y soporte técnico del equipo informático, la unidad solicitante deberá asegurarse de que las especificaciones y características técnicas del bien a adquirir sean las óptimas para el mejor funcionamiento, compatibilidad y desempeño de sus funciones de conformidad con la estructura informática instalada.

Capítulo III: Administración de Bienes Informáticos

1. Los empleados del CONSAA que por la naturaleza de su cargo y en el desempeño de sus funciones tengan bajo su responsabilidad programas, softwares y/o sistemas informáticos, a efecto de reducir los riesgos de fuga de información, ataque de virus o de cualquier otra amenaza que comprometa la seguridad de la información, deberán abstenerse de poner a disposición o conceder el uso a otros usuarios.

2. Si ocurriere algún evento que perjudique y comprometa el buen funcionamiento y seguridad de la red de datos de la institución, será de exclusiva responsabilidad de la jefatura inmediata de la unidad donde se violente esta disposición.

3. La Unidad Administrativa tiene la responsabilidad de informar oportunamente sobre ingresos, salidas y movimientos de personal a fin de mantener actualizada la nómina de usuarios que acceden a los servicios de la Institución tales como: correo electrónico, Internet, red de información y recursos.

4. Las unidades organizativas, deberán tener en sus computadoras su contraseña o password de entrada al sistema informático, el cual podrá ser actualizado cada seis meses para seguridad del usuario.

5. El sistema de redes inalámbricas WI-FI-Wireless del CONSAA, deberá estar protegido ante usuarios externos mediante una clave de acceso o password.

Solamente será autorizado por la Unidad Administrativa y la Dirección Ejecutiva el uso de redes inalámbricas a personas particulares.

1. El sistema de protección o seguridad de acceso al sistema de redes inalámbricas WI-FI-Wireless del CONSAA, deberá ser verificado por la Unidad Administrativa, cuando lo considere pertinente, con el apoyo técnico de la persona natural o jurídica encargada de brindar el mantenimiento preventivo, correctivo y soporte técnico al equipo informático del CONSAA.

Capítulo IV: Atención de requerimientos, mantenimiento preventivo, correctivo y soporte técnico de equipos informáticos

1. El mantenimiento preventivo, correctivo y soporte técnico de los equipos informáticos se realizará mediante la contratación de servicios externos, debiendo establecerse un programa permanente que permita diagnosticar posibles fallas, realizando además una limpieza en los equipos, respaldo de información y revisando que sean utilizados adecuadamente. La Unidad Administrativa será la responsable de vigilar y supervisar la adecuada y oportuna ejecución de los planes de mantenimiento preventivo.

2. No se autorizará la contratación de mantenimiento preventivo, correctivo y soporte técnico, a equipos que no sean propiedad del CONSAA o que estén en carácter de préstamo, es decir cuando un equipo de la institución esté en reparación externa y haya sido dejado otro equipo para cubrir la necesidad del usuario.

Capítulo V: Desarrollo de Sistemas Informáticos

1. Todos los sistemas y programas informáticos que sean desarrollados para la institución, deberán contar con el manual de uso, el dispositivo media instalador y las claves y llaves de ingreso, a efecto de que faciliten la resolución de problemas futuros.

2. Todo software que adquiera la institución deberá ser registrado y asignado en el control de activos intangibles que lleva la Unidad Administrativa, a través del Encargado de los mismos.

Capítulo VI: Uso Legal del Software

1. Cuando sea contratada la persona natural o jurídica para el mantenimiento preventivo, correctivo y soporte técnico, deberá elaborar un informe detallando los equipos informáticos del Consejo que cuentan con su

respectiva licencia original de uso de Microsoft Office. Será responsabilidad del jefe de la unidad donde se detecten equipos sin licencia, gestionar la compra del software respectivo.

2. Es responsabilidad de la Unidad Administrativa controlar que se cuente con las licencias de uso de los programas instalados en los equipos. Bajo ninguna circunstancia se procederá a la instalación de software si no se cuenta con respectiva licencia de uso.

3. Toda necesidad de instalación de nuevo software en los equipos, deberán ser justificados ante la Dirección Ejecutiva por la jefatura de la unidad correspondiente, para así proceder a su adquisición inmediata.

4. Todo el software catalogado como "freeware" o "shareware" que las unidades requieran descargar desde internet para ser instalados en sus computadores, deberán contar previamente con la autorización de la Dirección Ejecutiva y con la asesoría técnica del personal de informática contratado.

Capítulo VII: Administración de Usuarios, Correo Electrónico, Internet.

5. La Unidad Administrativa se apoyará en la persona natural o jurídica que presta los servicios de internet, web hosting y mantenimiento preventivo, correctivo y soporte técnico, para la administración de los servicios de Internet, correo electrónico, páginas Web, Antivirus, seguridad de la red de datos, recursos y otros.

6. Los empleados del Consejo, para mantener comunicación con los usuarios internos y externos, solamente podrán utilizar los correos electrónicos institucionales.

7. Únicamente los jefes de cada unidad podrán solicitar por escrito a la Dirección Ejecutiva, la creación de usuarios, cuentas de correo electrónico y otros.

8. La creación de cuentas de correo electrónico institucional dependerá de la disponibilidad de cuentas adquiridas y del espacio en los servidores de alojamiento. Caso contrario y mientras no sea resuelta la situación antes mencionada, el usuario interesado, previa autorización de su jefe inmediato, podrá utilizar correos electrónicos gratuitos en Internet, por ejemplo: yahoo, hotmail, gmail. Esto con la asesoría del personal de la persona natural o jurídica contratada para el mantenimiento preventivo, correctivo y soporte técnico. La administración, manipulación y modificación de dichas cuentas será de estricta responsabilidad del propietario.

9. La cuenta electrónica es personal e intransferible. El usuario es el único responsable directo de todas las acciones y mensajes que se lleven a cabo en su nombre. Esto incluye correo electrónico, acceso a sistemas y otros similares.

10. La suspensión total o parcial de los servicios al personal tales como: correo electrónico, navegación por Internet y otros, podrá ser solicitada por escrito a la Dirección Ejecutiva por la jefatura inmediata superior.

11. Se prohíbe hacer uso de Internet con fines de diversión, redes sociales, visitar páginas pornográficas, sitios de juegos, sitios de citas, apuestas electrónicas, sitios para descargar películas, música y programas. La Unidad Administrativa con apoyo de la persona natural o jurídica contratada para brindar el servicio de mantenimiento preventivo, correctivo y soporte técnico contratada, generarán reportes de aquellos usuarios que hayan violentado esta disposición y serán enviados a la jefatura inmediata superior para su conocimiento y sanción respectiva.

12. Se prohíbe proporcionar la contraseña del wifi a personas ajenas a la institución.

13. No se deben de descargar archivos de dudosa procedencia o correos marcados como spam (salvo el caso el correo se filtró en esa bandeja).

14. Al momento de enviar documentos por correo electrónico asegurarse de la dirección del destinatario y no enviar información a destinos equivocados, sobre todo cuando la información es delicada.

Capítulo VIII: Seguridad Física, Ambientación y Respaldos.

1. Las áreas donde se encuentre equipo de cómputo, deberán estar debidamente provistas con aire acondicionado a efectos de evitar recalentamientos que puedan generar falla, depreciación y bajo rendimiento de los equipos en cuestión.

2. El personal que tenga a su cargo equipo informático es responsable de:
   a) Velar de que se encuentran debidamente ventilados, sin obstrucciones, debidamente situados y que no existan objetos sobre los mismos.
   b) Que los equipos tales como el monitor, CPU, UPS, impresores y todo aquel periférico que utilicen para el desarrollo de las obligaciones diarias, queden

debidamente apagados al momento de retirarse de las instalaciones del CONSAA.

3. Los usuarios de los equipos informáticos de las correspondientes áreas o unidades son los responsables de mantener la información institucional debidamente ordenada para su posterior respaldo.

4. La empresa o persona natural encargada del mantenimiento preventivo, correctivo y soporte técnico informático contratada, realizará por lo menos una vez cada tres meses, los respaldos de información de cada usuario de la institución y al finalizar deberán ser entregados a la Unidad Administrativa.

5. El almacenamiento y custodia de los respaldos de información es responsabilidad de la Unidad Administrativa, la cual deberá protegerlos en un lugar seguro, seco y con restricciones de acceso, dentro de la Institución (caja fuerte, archivos con llave, escritorios con llave, etc.) que garantice el acceso, protección y seguridad de las mismas.

6. Todo dispositivo de almacenamiento extraíble (memorias USB, SD, Micro SD, otros), deberán ser debidamente analizados con el software antivirus asignado al equipo previo a su ejecución.

7. Es responsabilidad de la Unidad Administrativa garantizar la compra de antivirus para que los equipos de cómputo de la institución estén protegidos, y es responsabilidad del usuario correspondiente que en cada equipo se instale el antivirus correspondiente.

8. Los empleados usuarios que tengan asignados sistemas informáticos tienen la responsabilidad de resguardar el acceso a estos recursos con las contraseñas confidenciales que les fueron confiadas.

Elaborado por:	Revisado por:	Aprobado por:
Lic. Gerald Perdomo Zelaya CONSAA	Lic. Julio Angel Castro Luna Director Ejecutivo DIRECCION EJECUTIVA CONSAA CONSEJO SALVADOREÑO DE LA AGROINDUSTRIA AZUCARERA EL SALVADOR, C.A.	Directorio CONSAA según Acuerdo No. 400-8-2022 de fecha 21/09/2022