***Aprobado por la Dirección Ejecutiva el 30 de agosto 2021***

Agosto, 2021

**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**

|  |  |
| --- | --- |
| **OFICINA NACIONAL DE SEMILLAS** |  |

**INDICE**

[1. INTRODUCCION 2](#_Toc80785771)

[2. OBJETIVOS 2](#_Toc80785772)

[3. ALCANCE 3](#_Toc80785773)

[4. MARCO REGULATORIO Y NORMATIVO 3](#_Toc80785774)

[5. DEBERES INDIVIDUALES DE LOS USUARIOS DE LA INFORMACION 4](#_Toc80785775)

[6. DEBERES DEL DEPARTAMENTO ADMINISTRATIVO FINANCIERO 4](#_Toc80785776)

[7. DIRECTRICES RELACIONADAS CON EL MANEJO DE INFORMACIÓN CONFIDENCIAL 5](#_Toc80785777)

[8. USO ADECUADO DE SOFTWARE Y HARDWARE. 5](#_Toc80785778)

[9. CONTROL DE ANTIVIRUS 6](#_Toc80785779)

[10. CONTROL DE CONTRASEÑAS 6](#_Toc80785780)

[11. COPIAS DE RESPALDO DE INFORMACIÓN (BACK UP) 7](#_Toc80785781)

[12. DIRECTRICES RELACIONADAS CON EL DESARROLLO DEL SOFTWARE PARA LA OFICINA NACIONAL DE SEMILLAS 8](#_Toc80785782)

[13. POLÍTICAS DE SEGURIDAD EN EL ACCESO A ÁREAS RESTRINGIDAS 9](#_Toc80785783)

[14. POLÍTICA PARA UTILIZAR DEL CORREO ELECTRÓNICO INSTITUCIONAL 9](#_Toc80785784)

[15. ASESORÍA JURÍDICA 11](#_Toc80785785)

[16. TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES 12](#_Toc80785786)

[17. ADQUISICIÓN DE SOFTWARE Y HARDWARE EN CASOS DE EMERGENCIA NACIONAL Y COMPRAS A PROVEEDORES INTERNACIONALES 14](#_Toc80785787)

1. **INTRODUCCION**

La adopción de políticas, normas y procedimientos de seguridad de la información es una respuesta a la mejora del área de Tecnologías de Información y responde a los objetivos estratégicos de la misma, con el fin de definir a través del análisis, diseño e implementación de los objetivos, requisitos de seguridad, procesos, procedimientos, planes, políticas, controles, enfocados al tamaño, la tecnología y estructura de la misma.

En la actualidad la información para la Oficina Nacional de semillas (ONS), se reconoce como un activo muy valioso y en la medida que los sistemas de información apoyan cada vez más los procesos de misión y de apoyo, se requiere contar con respuestas de alto nivel que permitan el control y administración efectiva de la misma.

La implementación de las políticas busca reducir el riesgo de que en forma accidental o intencional se divulgue, modifique, destruya o use en forma indebida la información de la ONS y designan al área de tecnología de información y comunicación (TIC) como responsables de dictar la normatividad de la gestión de seguridad de la información, orientar y mejorar la administración de seguridad de los activos de información. Finalmente, también contempla el proveer las bases para el seguimiento y monitoreo en la entidad.

La Oficina Nacional de Semillas pretende mantener un esquema de seguridad que permita aseverar constantemente la confidencialidad, integridad y disponibilidad de la información. Para ello adopta, establece, implementa, opera, verifica y mejora un Sistema de Gestión de Seguridad de la Información (SGSI).

1. **OBJETIVOS**

**Objetivo General**

Establecer los lineamientos que permitan proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información y comunicación de la Oficina Nacional de Semillas, teniendo en cuenta los procesos, la operación, los objetivos de negocio y los requisitos legales vigentes en la Oficina Nacional de Semillas.

**Objetivos Específicos**

Definir la política de seguridad y privacidad de la información de la Oficina Nacional de Semillas.

Definir los lineamientos a ser considerados para diseñar e implementar el Sistema de Gestión de Seguridad de la Información alineado con las necesidades, los procesos, los objetivos y la operación de la Oficina Nacional de Semillas.

Colaborar con el cumplimiento a la normativa aplicable a la Oficina Nacional de Semillas en temas relacionados con las tecnologías de información y comunicación

Proteger los activos de información de la Oficina Nacional de Semillas.

Fortalecer la cultura de seguridad de la información en Oficina Nacional de Semillas, mediante la definición de una estrategia de uso y apropiación de la política.

1. **ALCANCE**

La política de Seguridad de la Información es aplicable en todo el ciclo de vida de los activos de información de la Oficina Nacional de Semillas, incluyendo creación, distribución, almacenamiento y destrucción. De igual forma para todos los funcionarios, contratistas y terceros que desempeñen alguna labor en la entidad. El alcance abarca desde el enunciado de la política, pasando por los lineamientos para la implementación del Sistema Seguridad y Privacidad de la Información, la matriz de riesgo, la definición de los indicadores para el monitoreo de cumplimiento de la política hasta la definición de una estrategia para la adopción de la política en la entidad.

1. **MARCO REGULATORIO Y NORMATIVO**

Política de seguridad de la información y comunicación de la Oficina Nacional de Semillas

**Política General**

Se define la Política de Seguridad de la Información como la manifestación que hace la Dirección Ejecutiva de la Oficina Nacional de Semillas, sobre la intención institucional de definir las bases para gestionar de manera adecuada y efectiva, la seguridad de la información; garantizando la confidencialidad, integridad y disponibilidad de sus activos de información.

La Oficina Nacional de Semillas pretende mediante la adopción e implementación de un Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información.

Adicionalmente se fomentará la cultura y toma de conciencia entre el personal (funcionarios, contratistas, proveedores y terceros) sobre la importancia de la seguridad de la información.

1. **DEBERES INDIVIDUALES DE LOS USUARIOS DE LA INFORMACION**
2. Usar la información de la Oficina Nacional de Semillas únicamente para propósitos autorizados y en cumplimiento de su labor.
3. Respetar la confidencialidad de la información de Oficina Nacional de Semillas.
4. No compartir perfiles de usuario, contraseñas, sesiones en estaciones de trabajo, documentos o cualquier tipo de información confidencial.
5. No anotar y/o almacenar en logares visibles las contraseñas de acceso a los sistemas.
6. Bloquear la sesión de la estación de trabajo al momento de ausentarse de la misma.
7. Está estrictamente prohibido utilizar software no licenciado en los recursos tecnológicos de la institución, copiar software licenciado de la Oficina Nacional de Semillas para utilizar en computadores personales y/o entregarlos a terceros.
8. **DEBERES DEL DEPARTAMENTO ADMINISTRATIVO FINANCIERO**
9. Informar las funciones de los usuarios, al área de Tecnologías de Información autorizando los niveles de acceso a la información.
10. Asegurar que los privilegios de acceso individuales reflejen una adecuada segregación de funciones. Un usuario no debe tener los permisos suficientes para originar, registrar y corregir/verificar una transacción sensitiva del negocio sin controles adecuados o una revisión independiente.
11. Definir el acceso del personal a aquellas áreas que hayan sido restringidas por razones de seguridad.
12. Los contratos con terceras personas, deben identificar claramente los acuerdos relacionados con la propiedad de la información y la no divulgación de información confidencial.
13. Cuando un funcionario se encuentra fuera de las funciones de la ONS, ya sea por licencia, permiso, suspensión, encargo, etc., el acceso a los recursos físicos y a la información debe ser inmediatamente suspendido por solicitud de su jefe inmediato, de ser necesario.
14. Cuando un funcionario finaliza relaciones (voluntaria o involuntariamente), se debe informar de manera inmediata al área de TI para:
15. Solicitar la revocación de los privilegios.
16. Revocar o restringir los privilegios de acceso antes de notificarle la terminación de sus funciones, si es apropiado.
17. Recoger los equipos, los dispositivos físicos y la revocación de las autorizaciones a los sistemas de información.
18. **DIRECTRICES RELACIONADAS CON EL MANEJO DE INFORMACIÓN CONFIDENCIAL**
19. Los documentos con esta información no pueden ser desatendidos, mal custodiados o inseguros.
20. Para la divulgación de acuerdo con los estándares de clasificación de la información, se requiere de autorización expresa de la jefatura correspondiente.
21. La divulgación de esta información, cualquiera que fuere su medio, verbal, escrita, telefónica o electrónica, debe ser efectuada sobre la base de la necesidad de conocerla de acuerdo a sus funciones.
22. Antes de divulgarse verbalmente información clasificada como Restringida o Confidencial debe indicarse su clasificación.
23. El acceso o distribución de información interna debe estar limitado a funcionarios u otros con la necesidad de conocerla o usarla para cumplir con sus funciones.
24. Se debe controlar el acceso a información confidencial que se encuentre almacenada; esto incluye información almacenada externamente o copias de respaldo.
25. **USO ADECUADO DE SOFTWARE Y HARDWARE**.

En las estaciones de trabajo de la Oficina Nacional de Semillas sólo se puede instalar software desarrollado o adquirido legalmente y cuya licencia de uso esté a nombre de la Oficina Nacional de Semillas.

La coordinación y ejecución de mantenimiento de programas o aplicaciones instaladas en las estaciones de trabajo corresponde a la unidad de Tecnologías de Información y Comunicación

Las estaciones de trabajo de la Oficina Nacional de Semillas deben ser utilizadas por los funcionarios únicamente para el desarrollo de las funciones normales de su trabajo.

Queda prohibido conectar equipos o elementos personales en la red institucional, para su uso únicamente se permite la conexión a la red denominada “Invitados”.

1. **CONTROL DE ANTIVIRUS**

Los equipos portátiles y estaciones de trabajo propiedad de la Oficina Nacional de Semillas deben mantener activo el antivirus, Sistema Operativo, Microsoft Office, licenciados y Actualizados y que su uso haya sido Autorizado.

Ningún usuario puede escribir, distribuir o introducir software que conozca o sospeche que tiene virus usando equipo de la Oficina Nacional de Semillas.

Cualquier información que venga por medio electrónico o magnético como correo electrónico o información de INTERNET, debe ser revisada por un software antivirus antes de ser descargada y utilizada.

El área de TI es responsable por la actualización oportuna del software antivirus.

El usuario debe asegurar que toda la información que es aceptada en la red interna de la ONS, provenga de fuentes conocidas.

1. **CONTROL DE CONTRASEÑAS**

El acceso a la información sensible de la Oficina Nacional de Semillas, aplicaciones y sistemas informáticos está regulado contra accesos no autorizados, requiriéndose, dentro del ámbito informático el uso de una clave de usuario y una contraseña para poder acceder a ella.

Los perfiles de usuario y la contraseña serán asignados individualmente para soportar el principio de responsabilidad individual por el área de TI

Los usuarios no pueden prestar su contraseña, lo que se realice con su perfil queda bajo total responsabilidad personal.

En ningún caso y por ninguna circunstancia el usuario no debe compartir, escribir o revelar su contraseña.

Las contraseñas deben cambiarse máximo cada 90 días. Si un sistema no obliga al cambio de contraseña, es responsabilidad del usuario realizar este cambio.

No se podrá repetir las contraseñas utilizadas anteriormente en los últimos cinco cambios.

Debe verificarse la identidad del usuario antes de que las contraseñas o perfiles de usuario sean habilitados nuevamente. Solo se puede cambiar una contraseña cuando el perfil de usuario pertenezca a quien solicita el cambio.

La identificación del usuario y su contraseña no deben ser iguales

Las contraseñas deben ser cuidadosamente seleccionadas para que no sean adivinadas fácilmente, por lo tanto, se deben tener en cuenta las siguientes recomendaciones.

No utilizar el primer o segundo nombre, los apellidos, el nombre del esposo, el nombre de sus hijos, etc., en ninguna forma (reversado, diminutivos, etc.)

No utilizar otra información personal fácil de obtener. Esto incluye: Placa o marca del carro, número del teléfono, marca, etc.

No se permitirá el uso de contraseñas que contengan sólo números o sólo letras.

Las contraseñas deberán contar con mínimo ocho caracteres; los mismos deberán ser alfanuméricos y deberá contener a menos un carácter en minúscula y uno en mayúscula.

Use contraseñas fáciles de recordar para que no tenga que escribirlas.

No use el nombre del perfil de usuario en ninguna forma como, por ejemplo: reversado o duplicado.

Cuando el área de TI asigne una contraseña; la misma siempre tendrá carácter de “temporal” y deberá ser cambiada por el usuario una vez realice su primer ingreso.

1. **COPIAS DE RESPALDO DE INFORMACIÓN (BACK UP)**

Se debe contar con un sistema automático para la recolección de copias de respaldo.

Las copias de respaldo deben tener el mismo nivel de protección de la información que poseen en su fuente original.

Los medios magnéticos que contienen información deben ser almacenados en lugares físicamente seguros.

Los medios magnéticos deben tener rótulos visibles y legibles tanto internos como externos.

Se debe mantener suficientes respaldos de la información para que en caso de contingencia se pueda recuperar la información oportunamente.

Todos los medios que contengan información clasificada como restringida o confidencial y que finalice su ciclo de vida, deben ser sobre escritos o destruidos; generándose el acta correspondiente.

Es responsabilidad del área de TI, mantener respaldo de la configuración del sistema operativo y de los servicios que estas proveen.

Las copias de seguridad, de todas las bases de datos de la institución se harán de forma completa y periódica a las 9 p.m. de lunes a viernes y un respaldo semanal los domingos a las 8 pm, sin excepción; estas se guardarán en la nube y se mantendrá por 12 días.

**Copias de seguridad de los equipos virtuales:**

Los equipos virtuales contienen una réplica de los datos de cada equipo de la institución; incluyendo los sistemas administrados por terceros; mismos que se respaldarán en discos externos diariamente en forma completa a las 8 pm. y adicionalmente se realizará un respaldo físico semanal los domingos a esa misma hora; mismas que se mantienen por un plazo de 7 días naturales.

Los sistemas que son administrados por un tercero (proveedor) deben aplicar esta política de seguridad y coordinar con el área de TI de la institución para garantizar un efectiva generación y manejo de los respaldos correspondientes.

1. **Directrices Relacionadas Con El Desarrollo Del Software Para la Oficina Nacional De Semillas**

En ningún caso el desarrollo de software interno y/o externo alterará, pasará por alto o comprometerá los mecanismos de seguridad definidos para una aplicación específica.

Los controles de seguridad incluidos en todo desarrollo deben ser documentados y deben permitir probar su efectividad.

Todas las aplicaciones desarrolladas deben contar con documentación funcional y técnica.

El área de TI de la Oficina Nacional de Semillas será la responsable de efectuar pruebas para asegurar que se han cumplido los requerimientos de seguridad.

Todo desarrollo y mantenimiento de software debe dejar las adecuadas pistas de auditoría (Registro de eventos).

Todas las aplicaciones desarrolladas y los archivos fuentes son propiedad de la Oficina Nacional de Semillas, así como las bibliotecas correspondientes para el buen funcionamiento del programa.

Las aplicaciones deben ser desarrollas en el lenguaje Visual Basic o C usando la base de Datos Microsoft SQL o la que se establezca de acuerdo a las necesidades institucionales y avances tecnológicos.

1. **Políticas de seguridad en el acceso a áreas restringidas**

El acceso a las áreas donde se procesa y almacena información de la Oficina Nacional de Semillas es clasificada como restringida o confidencial. Por lo que se requiere autorización de ingreso por el área de TI para aquellos que necesiten accederla.

Los servidores de aplicaciones y bases de datos, y otros dispositivos que son utilizadas para mantener funciones críticas del negocio, deben estar en un área de acceso restringido y separado del ambiente de las oficinas.

Las puertas exteriores del área de almacenamiento de información, deben ser cerradas con llave o estar aseguradas de otra forma durante las horas no hábiles.

Áreas diseñadas como restringidas deben también tener controles de acceso especiales. El acceso a estas áreas debe ser únicamente para autorizados.

Se controlará el ingreso de dispositivos móviles (Tablet, celulares, cámaras digitales, etc.) a las áreas catalogadas como restringidas.

No se permite la toma de fotografías dentro de estas áreas salvo a las áreas fiscalizadoras internas y/o externas.

Para el ingreso a las áreas restringidas deben solicitar permiso por escrito, indicando el motivo, sin este permiso debidamente autorizado no se le permitirá el ingreso.

Todo ingreso al área restringida debe ser supervisado por personal de TI.

1. **Política para utilizar del correo electrónico institucional**

La Dirección Ejecutiva o la Jefatura Administrativa Financiera son los únicos que podrán solicitara a TI la creación de correos tanto para funcionarios como para uso de un servicio especial.

La configuración del correo debe ser usando el servidor uk16.myserverhosts.com, con el servidor entrante (pop3) puerto 995 y el servidor de salida (SMTP) 465 usando la conexión cifrada SSL, con un tiempo menor de 30 días de respaldo en el servidor

Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de la Oficina Nacional de Semillas.

Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor

Todas las direcciones de correo electrónico deben ser creadas usando el estándar establecido por el La Oficina Nacional de Semillas (Primera letra del Nombre (s) y luego el Apellido).

Todos los funcionarios de la Oficina Nacional de Semillas tendrán correo electrónico Institucional.

El uso del correo electrónico es con fines Institucionales.

Se establecerá un tamaño de buzón de correo para cada usuario, es decir un espacio en disco en el servidor de correo, destinado al almacenamiento de mensajes electrónicos de cada usuario.

El usuario responsable del buzón deberá dar un trámite ágil al correo electrónico recibido, es decir, diariamente debe leer, responder y eliminar o archivar en el disco duro local, solamente los mensajes que soporten información relevante para el desarrollo de sus labores en la entidad.

Todos los mensajes que superen un (1) mes de almacenamiento en el servidor podrán ser eliminados permanentemente de acuerdo el espacio de almacenamiento y la limpieza del servidor. TI no se responsabiliza por el back up de los buzones de correo electrónico.

Ningún usuario deberá permitir a otro enviar correos utilizando su cuenta.

La asignación de cuentas de correo electrónico a trabajadores temporales será autorizada por el jefe del departamento Administrativo Financiero.

El cierre de cuentas de correo electrónico será autorizado por el jefe del departamento Administrativo Financiero.

El desvió de correo de un usuario a otro usuario se realizará únicamente cuando el propietario del correo lo autorice.

Apoyo de la Dirección Ejecutiva y Administración Activa

La Dirección Ejecutiva junto a la administración activa deben apoyar la seguridad de la información dentro de la entidad, definir un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información. Este compromiso se verá reflejado a través de:

Aprobando el plan estratégico del área de TI

Apoyando el cumplimiento de las políticas de seguridad de la información

Asignando responsabilidades "a las áreas y personas” asociadas a temas de la seguridad de la información.

Gestión de la Seguridad de la información

Las políticas deben ser revisadas una vez al año y en caso necesario se aplicarán los ajustes necesarios.

Se deben definir formalmente y comunicar todas las responsabilidades en cuanto a seguridad de la información, con los funcionarios de la institución.

1. **Asesoría Jurídica**

Debe incluir y tener en cuenta los lineamientos y políticas de Seguridad de la información en la gestión de la contratación con terceros, proveedores y contratistas.

Es responsabilidad de esta dependencia velar por el cumplimiento de la política de seguridad de la información en el desarrollo de sus funciones, con sus funcionarias contratistas, proveedores y con terceros. Así mismo, asesorar en materia legal a Oficina Nacional de Semillas en lo que se refiere a la seguridad de la información.

Esta área, debe exigir para todo contrato con proveedores, terceros, contratistas, etc., la firma del acuerdo de confidencialidad y apoyar la supervisión del cumplimiento de las políticas de Seguridad de la Información.

1. **Tecnologías de Información y Comunicaciones**

Tecnologías de Información y Comunicaciones, debe cumplir la función de cubrir los requerimientos de seguridad de la información, definidos para la operación, administración y comunicación de los sistemas y recursos de tecnología.

Todas las nuevas adquisiciones e instalaciones de soluciones o plataformas tecnológicas (Hardware o software), deben contar la asesoría técnica de TI, considerando aspectos de viabilidad técnica, compatibilidad, capacidad, integridad, disponibilidad y confidencialidad.

Asesorar en la aplicación de la metodología para el mantenimiento de los planes de contingencia y continuidad del negocio.

Evaluar, seleccionar e implantar herramientas que faciliten la labor de seguridad de la información

Dar los lineamientos para controlar el acceso a los sistemas de información y la modificación de privilegios

Mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes

Realizar estudios o consultas de pruebas de seguridad en todos los ambientes informáticos de la institución.

Gestionar los Riesgos identificados; y de sus respectivos planes de tratamiento. Evaluación de riesgos residuales.

Revisar y actualizar periódicamente los inventarios de activos de información.

Documentar por medio de acta y ante la auditoría interna cualquier retiro de activo de TI

Funcionarios - Contratistas - Proveedores - terceros

Los usuarios de la información (funcionarios - contratistas - proveedores - terceros) y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer y cumplir la Política de Seguridad de la Información vigente.

Los funcionarios - contratistas - proveedores - terceros, deben:

Conocer, comprender y aplicar la Política de Seguridad de la información en los procedimientos que apliquen a su trabajo.

Llevar a cabo su trabajo, asegurándose de que sus acciones no producen ninguna infracción de seguridad de la información.

Comunicar las incidencias de seguridad de la información que detecte a TI.

Cumplir con el acuerdo de confidencialidad firmado con la institución.

Hacer uso de las mejores prácticas definidas en la entidad para todos los temas relacionados con la seguridad de la información.

Responsables de la Información

El propietario de un activo de información, entendiéndose como tal, aquel que es el responsable de dicho activo, tendrá las siguientes responsabilidades:

Atender en toda su extensión la presente política.

Informar al área de TI cuando detecte cualquier incidente de seguridad de la información, para tratarlo y corregirlo mediante la aplicación de controles.

En los casos que aplique, firmar cláusulas de confidencialidad en sus contratos; para dejar claro el compromiso.

Conocer, comprender y aplicar la Política de Seguridad de la información en los procedimientos que apliquen a su trabajo.

Administradores de los Sistemas o Plataformas de TI.

Los administradores de los diferentes sistemas o de las diferentes plataformas de TI, deben:

Conocer y cumplir las políticas de seguridad de la información.

Conocer, comprender y aplicar la Política de Seguridad de la información, en los procedimientos que apliquen a su trabajo.

Dentro de sus funciones de la administración de los sistemas de información o plataformas tecnológicas, aplicar los lineamientos o políticas de seguridad de la información que le sean comunicadas.

Informar oportunamente al Jefe Inmediato cuando detecte cualquier incidente de seguridad de la información y sugerir controles o contramedidas para su tratamiento.

Documentar los aspectos de seguridad de la información aplicados dentro de su línea de gestión y su respectivo control de cambios.

Mantener actualizados a los usuarios internos de la institución sobre seguridad de TI para fortalecer la operación institucional.

Para la adquisición de nuevos desarrollos por parte de la institución, TI deberá generar la justificación técnica sobre el lenguaje de programación que se utilizará.

Para la implementación de software externo por requerimiento de normativa y/o órganos fiscalizadores; TI deberá emitir criterio sobre la posibilidad de integración con los sistemas internos relacionados, para tratar de eliminar el reproceso.

Para cualquiera de los casos anteriores TI tendrá un plazo máximo de 15 días hábiles para emitir su criterio.

1. **Adquisición de Software y Hardware en casos de emergencia nacional y compras a proveedores internacionales**

En caso de emergencia nacional o de requerirse compra de software o hardware cuyo proveedor no se encuentre domiciliado en el país, se aplicará la compra correspondiente atendiendo la normativa aplicable; para tales efectos TI generará la justificación técnica del requerimiento.