Documento de Seguridad de la Información

Título de la *Norma*	Documento de Seguridad de la Información
Ámbito geográfico	Nacional
Categoría	Procedimiento
Fecha de aprobación	13 de junio 2020
Órgano de aprobación	Patronato

1. Objeto

El Documento de Seguridad de la Información recoge las normas de uso adecuado y los términos y condiciones de utilización de los sistemas y activos de información de **FUNDACIÓN AENILCE**.

2. Alcance

Los requisitos establecidos en este procedimiento afectan a todo el personal, socios de negocio y proveedores de **FUNDACIÓN AENILCE** que hacen uso de los sistemas y activos de información de **FUNDACIÓN AENILCE**.

3. Términos y Definiciones

- **RGPD**.: Reglamento General de Protección de Datos UE 2016-679, DOUE de 27 de abril de 2016.
- **LOPDGDD:** Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales.
- **INFORMACIÓN:** Conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

4. Clasificación de la información

Con el fin de asegurar que la información recibe un nivel adecuado de protección, se clasifica en: confidencial, interna y pública.

Esta protección se aplica para toda la información que se genere o se tenga acceso, con el fin de controlar el tratamiento que se realiza y verificar la autorización de acceso, además de proporcionar un nivel adecuado de protección en función del tipo de información de que se trate.

4.1 Información Confidencial. Acceso Restringido

Es aquella información que sólo debe estar disponible para las personas o áreas internas autorizadas, estando prohibida su difusión sin autorización previa del superior inmediato.

4.2 Información Interna. Acceso libre

Es aquella información que puede conocer y divulgar libremente cualquier empleado, a través de los sistemas de la organización.

El acceso a este tipo de información sin autorización podría causar pequeños daños a la entidad, tales como incomodidad por su revelación, pero en ningún momento esto supondría un daño económico o reputacional. El uso de la información interna no puede ser desvelado a personal no autorizado o terceros fuera de la entidad, sin la correspondiente autorización.

4.3 Información Pública

Es aquella información que se puede divulgar libremente tanto a nivel interno como a nivel externo de **FUNDACIÓN AENILCE**. Está disponible para cualquier persona que la solicitara sin ningún tipo de restricciones.

5. Protección de la información

La siguiente tabla contiene las medidas de protección aplicables en función del nivel de la información.

Nivel	*Medidas de protección*
Información Pública.	• La información podrá almacenarse en cualquier soporte o en cualquier parte del sistema, accesible por el propio usuario. • Para la destrucción de documentos en formato papel se emplearán los contenedores de permitan su reciclaje.
Información Interna. Acceso libre.	• El acceso deberá estar controlado. • Se podrá almacenar la información en un directorio o repositorio interno. • Se deberán realizar copias de seguridad. • El acceso a los repositorios deberá estar restringido. • La destrucción se llevará a cabo mediante mecanismos que impidan la recuperación de la información.
Nivel	*Medidas de protección*
Información Confidencial. Acceso restringido.	• El acceso se restringe a personal debidamente autorizado. • Estará almacenada en un espacio lógico de la red, con control de acceso al mismo. • Se deberán realizar copias de seguridad. • Solamente el personal autorizado al acceso de esta información podrá acceder a la recuperación de los datos. • Se prohíbe el almacenamiento de este tipo de información en soportes sin medidas de seguridad y sin autorización. • Para el envío de la información fuera de **FUNDACIÓN AENILCE** se deberá contar con autorización previa. • La destrucción se llevará a cabo mediante mecanismos que impidan la recuperación de la información. • Se requerirá trazabilidad si se realiza un mal uso de la información.

6. Uso responsable de los Recursos

6.1. Uso responsable de los sistemas de información

Los sistemas de información son un activo valioso para **FUNDACIÓN AENILCE** y se deberá hacer un uso de ellos de forma responsable. En este sentido, todo trabajador en el ejercicio de sus funciones deberá tener en cuenta las siguientes recomendaciones para su uso adecuado:

- El uso de los sistemas de información queda restringido al ámbito profesional.
- Ningún usuario instalará software no autorizado en su equipo, especialmente software protegido por derechos de autor, sin la correspondiente licencia de uso adquirida por **FUNDACIÓN AENILCE**.
- No se podrá modificar la configuración de los activos sin previa autorización.
- Los trabajadores que utilicen sistemas de información compartidos deberán cerrar todas las aplicaciones y desconectarse de su sesión al finalizar la jornada laboral.
- El tratamiento de la Información que contenga datos de carácter personal deberá seguir lo estipulado en el RGPD y la LOPDGDD.

6.1.1. Equipo desatendido

Los trabajadores deberán apagar sus equipos al finalizar la jornada laboral. **FUNDACIÓN AENILCE** se reserva el derecho a forzar el apagado de los equipos al finalizar la jornada laboral o cuando lo considere justificado.

Los equipos están configurados para su bloqueo automático pasados 20 minutos de innegocio, para así mantener la información fuera del alcance de terceras personas cuando el equipo esté desatendido.

6.1.2. Puesto de trabajo despejado

Cuando el trabajador se ausente del puesto de trabajo, la documentación debe recogerse y almacenarse en armarios o cajoneras cerradas.

6.1.3. Contenidos del puesto de usuario

Se dispondrá en el equipo de usuario únicamente de los productos software corporativo y de aquellos otros productos a que esté autorizado ese usuario en virtud de sus necesidades.

6.1.4. Uso de soportes extraíbles

Con objeto de proteger la información contenida en los activos se toman las siguientes medidas sobre el uso de soportes extraíbles (memorias USB, disco duros externos, CDs, DVD´s, etc.):

- El personal de **FUNDACIÓN AENILCE** tiene permitido el uso de soportes extraíbles para almacenar información clasificada como **interna** y **pública** cuando lo considere necesario en la realización de sus actividades de trabajo.

- El personal de **FUNDACIÓN AENILCE** tiene prohibido el uso de soportes extraíbles para almacenar información clasificada como **confidencial**, salvo que haya sido autorizado.

6.1.5. Código malicioso en servidores

Actualmente, se dispone de herramientas contra códigos maliciosos que proporcionan protección antivirus, antispyware y antispam en los servidores, que se mantiene actualizada periódicamente; no obstante, en caso de detectarse una incidencia, deberá comunicarse al Departamento de Informática.

6.1.6. Uso de contraseñas

Cada trabajador es responsable de sus contraseñas, tanto de su salvaguarda como de su elección y **no deberá cederlas ni dejarlas visibles**, es por ello por lo que:

- No dirá a nadie sus contraseñas ni las conservará por escrito.
- Cambiará sus contraseñas cuando sospeche que han podido ser vulneradas.

- Para garantizar la seguridad y robustez de las contraseñas de acceso es necesario que los empleados las cambien cada 180 días, aplicando las siguientes directrices:
    - Longitud mínima de 8 caracteres.

6.1.7. Protección Antivirus

Todos los equipos disponen de una herramienta instalada que los protege contra virus, troyanos, spyware, entre otros, y se mantiene actualizada periódicamente; no obstante, en caso de detectarse una incidencia, deberá comunicarse al Departamento de Informática.

6.2. Uso responsable del correo electrónico

- El correo electrónico deberá ser usado para la comunicación de cuestiones relativas a la negocio laboral y/o cumplimiento de las obligaciones al respecto.
- Los trabajadores no deben acceder ni divulgar el correo de otros usuarios sin el consentimiento previo de estos.
- La configuración de las cuentas de correo se establecerá para cada usuario en función de sus necesidades de trabajo.
- No se deberá distribuir o divulgar cualquier asunto, material o información que fomente la discriminación, la violencia o el odio hacía una persona o colectivo por razón de sexo, raza, religión o nacionalidad, así como cualquier otra información o asunto que sea difamatorio, obsceno, inmoral o ilícito.
- Por motivos de seguridad se debe evitar abrir correos desconocidos o no fiables aunque hayan pasado por los mecanismos de protección, en especial si contienen ficheros adjuntos potencialmente peligrosos (extensiones del tipo .exe, .bat, .vs*, .com, etc.). estos correos deben adjuntarse al Departamento de Sistemas.

6.3. Uso responsable del acceso a Internet

- No se deberá acceder a páginas que puedan poner en peligro los sistemas de información pertenecientes a **FUNDACIÓN AENILCE**.
- No se difundirá a través de internet *Información Confidencial* o información que pueda causar algún perjuicio a la misma.
- Se recomienda no realizar trasferencia de ficheros a través de internet (mediante plataformas públicas de libre acceso como WeTransfer)

6.4. Reporte de Incidencias

Todo el personal, durante la ejecución de sus funciones, permanecerá atento a sucesos inesperados o poco comunes, tales como:

- Extravío o robo de equipamiento.
- Evidencia o sospecha de alteración de permisos de acceso o contraseñas de acceso de usuarios.
- Comportamientos anómalos en los sistemas de información.
- Configuraciones desconocidas en los sistemas de información.
- Evidencia o sospecha de acceso o modificación no autorizada de información.
- Hallazgo de información en ubicaciones no designadas para ello.

6.5. Retirada y Salida de material Informático

No está permitido la retirada o salida de material informático de las instalaciones de **FUNDACIÓN AENILCE**, sin contar con la debida autorización del superior inmediato.

6.6. Conexiones a través de VPN para teletrabajo

Aquellos usuarios que posean permisos para conectarse a través de la VPN para teletrabajo deberán:

- No instalar el software de VPN en un ordenador del cual no se tenga la certeza de que está libre de malware, virus, spyware o que sea de uso compartido.
- No seleccionar la opción de recordar contraseña en ningún sistema o sitio Web.
- Los usuarios deben aplicar las indicaciones del punto 7.1.6 para el uso de contraseñas.
- Los usuarios deben activar un salvapantallas protegido por contraseña si utiliza un ordenador no corporativo.

6.7. Acceso remoto a escritorio de usuario

El personal técnico del Departamento de Informática realizará exclusivamente la conexión remota al escritorio de un equipo, que requerirá siempre la aceptación expresa por parte del usuario del mismo.

6.8. Reutilización y Eliminación de soportes de Información

Los soportes que almacenen información y vayan a ser reutilizados para otros fines o retirados al finalizar su ciclo de vida, deberán ser previamente tratados para evitar fugas que comprometan la confidencialidad de la información.

A continuación, se describen los métodos a emplear para el tratamiento de soportes o dispositivos de **FUNDACIÓN AENILCE** que son retirados o reutilizados:

- Borrado de los discos duros.
- Destrucción del soporte para CDs y DVDs.
- Destrucción de soporte papel a través de máquinas de destrucción de papel o contenedores específicos habilitados para esta finalidad para su posterior recogida y destrucción por empresa que emite certificación de eliminación segura.
- Servidores, dispositivos de comunicaciones y móviles: eliminación del contenido de información con el borrado seguro de datos.
- Dispositivos de usuario (PCs, discos duros, tarjetas de memoria): Los datos del usuario se retendrán durante 15 días. Pasado ese tiempo, se procederá al borrado seguro de los datos.
- Los usuarios deberán proceder a la destrucción de las copias o reproducciones desechadas, de forma que se evite el posterior acceso a la información contenida en las mismas o su recuperación posterior.

6.9. Traslado de información

Siempre que se proceda al traslado físico de soportes o documentos, deberán adoptarse medidas que impidan el acceso o manipulación de la información objeto de traslado:

a. Todas las operaciones de recogida, transporte y entrega de documentación deben ser realizadas por personal debidamente autorizado.
b. La documentación se transportará en un maletín, porta documentos o similar, valija o mensajería.
c. La documentación debe ser llevada directamente al lugar donde esté prevista su entrega o depósito.
d. En la documentación quedará especificado el Remitente y el Destinatario.

7. Control del acceso lógico

Según las funciones o puesto de trabajo de la persona se le asignará un perfil y permisos de acceso, que permitirá identificar al usuario en todos los equipos a los que acceda.

Para acceder a cualquiera de los equipos, los usuarios necesitan entran en el dominio con su identificación y contraseña, que son verificados por el sistema informático, permitiéndole acceder a los servicios, carpetas y directorios que tenga asignados.

La posibilidad de intentar reiteradamente el acceso no autorizado al Dominio y/o aplicación informática, estará limitada mediante un sistema que impedirá realizar más de cinco intentos fallidos de forma consecutiva.

7.1. Alta Usuarios

Cuando se aprueba una nueva contratación se comunica al Departamento de Informática la información del candidato para que efectúe la tramitación del alta de usuario de correo, el acceso a red y herramientas administrativas.

Si el trabajador tuviera asignado algún equipo, se dejará constancia en el Registro de Activos. Se dispondrá en el equipo de usuario únicamente de los productos de software corporativo y de aquellos otros productos a que esté autorizado ese usuario.

7.2. Baja Usuario

La solicitud de baja se realiza enviando al Departamento de Informática una solicitud por correo electrónico indicando el trabajador y la fecha de baja.

A continuación, se cursará la baja de la solicitud accediendo al Registro de Activos y eliminando sus permisos asociados una vez que haya terminado el periodo posterior de retención de 15 días, aunque la cuenta estará bloqueada durante todo ese tiempo.

7.3. Bloqueo de cuentas.

Las cuentas de usuario deben estar configuradas de modo que se bloqueen automáticamente tras cinco intentos fallidos de validación de la contraseña.

Además, también se podrán bloquear de oficio una cuenta de usuario en el caso de investigación de un incidente de seguridad o cuando existan sospechas de que la cuenta está siendo usada para actividades irregulares.

Por otro lado, cuando una cuenta de acceso no haya sido usada por un periodo superior a 90 días, será bloqueada automática o manualmente.

7.4. Usuarios genéricos.

Se entiende por cuentas de usuarios genéricos todas aquellas que requieren ser compartidas por dos o más personas que realizan actividades comunes, siempre que no se ponga en riesgo la seguridad de la información.

Todos los usuarios genéricos tendrán un propietario, que será el responsable de las acciones que se realicen con el mismo.

8. Copias de respaldo y recuperación

El personal laboral comparte archivos a través del servidor de **FUNDACIÓN AENILCE**, del cual se hará backup con la siguiente frecuencia:

- Copias diarias completas a final del día, de lunes a jueves (4 copias) se guardarán durante una semana.
- Copia del viernes para su envío al edificio alternativo (1 copia) se guardarán durante una semana.
- Copias semanales completas al final de cada viernes (4 copias) se guardarán durante un mes.
- Copias mensuales el primer sábado de cada mes, se guardarán durante 24 meses.

9. Términos y Condiciones

En este apartado se establecen los términos y condiciones que reflejan la responsabilidad en lo relativo a la seguridad de la información en función de cuál sea su relación con **FUNDACIÓN AENILCE**.

9.1. Personal laboral

El personal laboral se regirá por la legislación que aplique en el momento concreto. Además de cumplir el régimen disciplinario correspondiente, el personal laboral deberá conocer y aceptar las cláusulas indicadas en el contrato de trabajo respecto al deber de confidencialidad.

A este respecto, todo trabajador queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento de su función, especialmente la *Información Confidencial*.

Esta obligación subsistirá, incluso, una vez finalizada la relación laboral en **FUNDACIÓN AENILCE**.

9.2. Socios de actividad y Proveedores

Las personas que presten servicios a **FUNDACIÓN AENILCE** deberán firmar las cláusulas de confidencialidad y respetar las medidas de seguridad de los sistemas de información de **FUNDACIÓN AENILCE**.

La información es uno de los principales activos de cualquier organización y todo socio de actividad y proveedores tienen la obligación de guardar secreto sobre aquellos documentos que contengan información relevante sobre aspectos internos de **FUNDACIÓN AENILCE**.