INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

OFICINA TÉCNICA DE INFORMÁTICA

POLÍTICA

"POLÍTICA DE CLASIFICACIÓN, MANEJO Y DIFUSIÓN DE LA INFORMACIÓN EN LA OTIN"

Código: POL-003-OTIN-2018
Versión 1.0.0

POLITICA		
NOMBRE DE LA POLITICA: POLITICA DE CLASIFICACIÓN, MANEJO Y DIFUSIÓN EN LA INFORMACIÓN EN LA OTIN		
CODIGO: POL- 003 -OTIN-2018		**VERSION: 1.0.0**
PROCESO AL QUE PERTENECE: Gestión de Seguridad de la Información		
Elaborado por: Unidad Funcional de Calidad, Procesos y Seguridad de la Información	**Revisado por:** Unidad Funcional de Calidad, Procesos y Seguridad de la Información	**Aprobado por:** Director Técnico de la Oficina Técnica de Informática - OTIN
Nombre: Luis Taype Ignacio	**Nombre:** Franklin Arias Moreno	**Nombre:** Manuel Matos Alvarado
Fecha:	**Fecha:**	**Fecha:**
Firma	**Firma**	**Firma**

Información del Documento

Fecha de Creación:	Código:	Versión:	Elaborado por:	Aprobado por:
21/09/2018	POL-003-OTIN-2018	1.0.0	Emilia Berroa Buendía Luis Taype Ignacio	Manuel Amador Mattos Alvarado - Director Técnico de la Oficina Técnica de Informática - OTIN

Historial del Documento

Fecha de Creación:	Versión:	Modificado/Creado por:	Descripción de la modificación:
21/09/2018	1.0.0	Emilia Berroa Buendía Luis Taype Ignacio	Creación del primer documento

TABLA DE CONTENIDO

"POLÍTICA DE CLASIFICACIÓN, MANEJO Y DIFUSIÓN DE LA INFORMACIÓN EN LA OTIN"

1. OBJETIVO

Establecer los lineamientos y disposiciones para una adecuada clasificación y manejo de la información en un nivel adecuado dentro de la Oficina Técnica de Informática, con el fin de salvaguardar su confidencialidad y asegurar su correcta difusión, en forma veraz, transparente, equitativa y oportuna.

2. ALCANCE

La presente política se aplica a toda la información bajo custodia de la Oficina Técnica de Informática, incluyendo la que se encuentra dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) del INEI; es decir a todos los tipos de información, independientemente del formato en que se encuentre.

3. ÁMBITO DE LA APLICACIÓN

Las disposiciones de la presente política tienen el carácter de obligatorio y serán aplicables a todas aquellas personas que presten sus servicios o tengan algún tipo de relación con la Oficina Técnica de Informática, y que en el desarrollo de sus actividades puedan acceder a la información.

4. MARCO LEGAL Y/O NORMATIVO

- NTP-ISO/IEC 27001:2014, puntos A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3
- Ley N°27806 y sus modificaciones – Ley de transparencia y acceso a la información pública
- Ley N°29733 y sus modificaciones – Ley de protección de datos personales
- Ley N° 27658, Ley de Modernización de la Gestión del Estado.
- Estándar en materia de Seguridad de la Información ISO/IEC 27002:2013;
- Código de buenas Practicas Estadísticas, aprobado con R.J. Nº 237-2014-INEI
- COBIT v. 5.0 en lo referente a seguridad de la información.
- Política de Seguridad de la información

5. ABREVIATURAS Y DEFINICIONES

5.1. ABREVIATURAS

- **CISO** : Oficial de Seguridad de la Información
- **OTIN** : Oficina Técnica de Informática
- **SGSI** : Sistema de Gestión de Seguridad de la Información

5.2. DEFINICIONES

- **Activo:** Cualquier cosa que tiene valor para la organización NTP-ISO /IEC 27001
- **Activo de Información:** Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información con valor para la Institución.
- **Colaborador:** Persona física que labora para la OTIN, sin distingo de régimen laboral o contractual o de nivel jerárquico que tenga acceso a la información.
- **Gestión de la Información:** se refiere a un ciclo de actividad organizacional: la adquisición de información de una o más fuentes, la custodia y la distribución de esa información a aquellos que la necesitan, y su disposición final a través del archivado o borrado.
- **Información:** Corresponde al conjunto de datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, entre otros.
- **Nivel de Clasificación de la Información:** Es el estatus con el que se clasifica cualquier tipo de información.
- **Propiedad de los activos:** los activos de información del inventario deben tener un propietario.
- **Propietario de la Información:** Persona que tiene poder de decisión sobre la información, ya sea porque le pertenece, porque corresponde al ámbito de su competencia, o porque le ha sido formalmente asignado.
- **Registro de activos de Información:** Es el inventario de la información.
- **Responsable de la producción de la Información:** Corresponde al nombre del área, dependencia o unidad interna que creo la información.
- **Responsable o custodio de la Información:** Corresponde al nombre del área, dependencia o unidad interna encargada de la custodia o control de la información para efectos de permitir su acceso.

6. PRINCIPIOS QUE RIGEN LA POLÍTICA

Los siguientes principios constituyen los fundamentos sobre lo que se basará cualquier acción en materia de seguridad de la información:

- **Confidencialidad**
  Los activos de la información deben mantenerse protegidos para asegurar la confidencialidad y privacidad entre usuarios con acceso autorizado a los mismos. En todo momento deben mantenerse esquemas de seguridad que prevengan la divulgación no autorizada de información.

- **Disponibilidad**
  Los activos de información deben estar disponibles para su uso por parte de los usuarios autorizados toda vez que lo requieran, garantizando el acceso oportuno a la información y a los recursos relacionados con la misma.

- **Integridad**
  Los activos de la información deben estar adecuadamente protegidos para asegurar su integridad. Las medidas de validación definidas deben permitir detectar la modificación inadecuada, adulteración o eliminación de los activos de información.

- **Propiedad**
  La información registrada, almacenada y procesada por las operaciones de la organización es propiedad del INEI, a menos que en una relación contractual se establezca lo contrario, y la facultad de otorgar acceso a ella es del propietario de la información.

- **Protección**
  Los activos de información deben ser protegidos con el nivel de seguridad necesario, guardando proporción entre el valor y el riesgo de pérdida para el INEI. La protección debe enfocarse en la confidencialidad, integridad y disponibilidad de estos activos.

- **Uso apropiado**
  Los activos de la información disponibles en el INEI deben ser utilizados en forma adecuada, eficiente, racional y exclusivamente para el desarrollo de las actividades institucionales.

7. POLÍTICAS

7.1. CONSIDERACIONES GENERALES

- La clasificación de la información, está basada en la confidencialidad como principio rector e incluye el manejo de la información en cuanto a la confidencialidad, la integridad y la disponibilidad, así mismo contempla el impacto que causaría la perdida de alguna de estas propiedades.

7.2. PASOS Y RESPONSABILIDADES

Para realizar una buena gestión de la información se siguen los siguientes pasos:

Paso	Responsable
1. Incluir la información en el Inventario de Activos	[cargo - proveedor del activo]
2. Clasificación de la información	Propietario de la información
3. Etiquetado de la información	Propietario de la información
4. Manejo de la información	Personas que poseen derechos de acceso

Si la información clasificada proviene de fuentes externas a la OTIN, el [cargo - proveedor del activo] es el responsable de su clasificación según las reglas establecidas en esta Política, y esta persona se convierte en el propietario de ese activo de información.

7.3. INVENTARIO DE LA INFORMACIÓN

- Se establecerá un inventario de los activos de información disponible en la OTIN, considerando registrar aspectos tales como el: tamaño, ubicación, servicios, dependencia o unidad interna a los que pertenecen, así como quien es el responsable de la misma. El inventario permitirá identificar los activos de información a los que se les debe brindar mayor protección.

- La información de la OTIN podemos tenerla en distintos formatos y medios, como:

  - ✓ Documentos en Papel
  - ✓ Documentos Electrónicos
  - ✓ Sistemas de Información
  - ✓ Correo Electrónico
  - ✓ Soporte de almacenamiento electrónico
  - ✓ Información transmitida oralmente

- El inventario debe ser actualizado periódicamente por la Unidad Funcional responsable de la custodia de la Información, cada vez que se realice alguna adición o eliminación de los activos. Las coordinaciones sobre el inventario serán propiamente exclusivas con la oficial de Seguridad de la Información – INEI.

7.4. CLASIFICACIÓN DE LA INFORMACIÓN

7.3.1 Criterios de clasificación de la información

- Los criterios de clasificación se aplicarán a todo tipo de información generada en la OTIN y/o se encuentre bajo su custodia, adquirida o administrada, en medios electrónicos, escritos, entre otros. La clasificación y controles de protección asociados a la información se establecen de acuerdo a las necesidades específicas de la Institución con respecto a la distribución (uso compartido) o restricción de la información, así como las obligaciones de resguardo de información.

- El nivel de confidencialidad se determinará de acuerdo a los siguientes criterios:

  - ✓ Valor de la información
  - ✓ Sensibilidad y grado crítico de la información
  - ✓ Obligaciones legales y contractuales

7.3.2 Niveles de clasificación de la información

- Toda la información de la OTIN deberá ser clasificada en niveles de confidencialidad, el cual se hará en base a los resultados obtenidos tras la evaluación del riesgo:

Nivel de Confidencialidad	Etiquetado	Criterios de Clasificación	Restricción de Acceso
CONFIDENCIAL	Etiquetar	El acceso no autorizado a la información podría dañar de forma catastrófica (irreparable) y/o perjudicar a la OTIN.	La información está disponible previa autorización por parte del Director Técnico y/o para un grupo específico de colaboradores, que ejercen funciones definidas, teniendo en cuenta la confidencialidad para mayor protección. Además respecto a datos personales se toma en cuenta la Ley N°29733.- **Ley de protección de datos personales.**

RESTRINGIDO	(Sin etiquetar)	El acceso no autorizado a la información podría dañar y/o implicar un impacto no deseado a la OTIN.	La información está disponible para un grupo específico de colaboradores de la OTIN y de terceros autorizados. La información se caracteriza por ser información altamente sensible.
USO INTERNO	(Sin etiquetar)	El acceso no autorizado a la información podría ocasionar daños y/o inconvenientes menores a la OTIN.	La información está disponible única y exclusivamente de uso de los colaboradores de la OTIN y terceros seleccionados
PUBLICO	(Sin etiquetar)	Hacer pública la información no pude dañar a la OTIN de ninguna manera.	La información está disponible para todo el público, puede ser compartida sin ninguna restricción, ya que su difusión no implica que los intereses de la OTIN pudieran ser perjudicados.

7.3.3 Lista de personas autorizadas

- La información clasificada como **"Confidencial"** y **"Restringida"** debe estar acompañada de una lista de personas autorizadas en la que el propietario de la información específica quiénes tienen derechos de acceso a esa información, posteriormente estas personas tendrán que firmar una declaración de confidencialidad (Anexo I), que será dirigido vía correo electrónico al propietario de la información en formato digital para su custodia ante cualquier eventualidad que tenga que ver con la información.

- Para la información clasificada como **"Pública"** no se requiere establecer las personas autorizadas para acceder a la información.

7.3.4 Reclasificación

- Los propietarios de la información deben validar el nivel de confidencialidad de los activos de información al menos cada año y evaluar si se puede cambiar dicho nivel. Si es posible, deberán bajarlo.

7.5. ETIQUETADO DE LA INFORMACION

- En la OTIN, el propietario de la información asignará el etiquetado exclusivamente a la información clasificada como **"Confidencial"**, independiente del formato en que se encuentre. Además, tendrá que seguir una serie de pautas de acuerdo al tipo de formato:

  - ✓ **Documentos en Papel:** El nivel de confidencialidad se indica en la esquina superior derecha de cada página del documento; también se indica en la portada o en el sobre que contiene dicho documento, como también en la carpeta de archivo en la que se guarda el documento.

  - ✓ **Documentos Electrónicos:** El nivel de confidencialidad se indica en la esquina superior derecha de cada página del documento.

  - ✓ **Sistemas de Información:** El nivel de confidencialidad en aplicaciones y bases de datos debe ser indicado en la pantalla de acceso al sistema, como también en la esquina superior derecha de cada pantalla consecutiva que muestra información confidencial.

  - ✓ **Correo Electrónico:** Se indica el nivel de confidencialidad en la primera línea del cuerpo del correo electrónico.

  - ✓ **Soporte de almacenamiento electrónico:** Se debe indicar el nivel de confidencialidad sobre la superficie de cada soporte.

  - ✓ **Información transmitida oralmente:** El nivel de confidencialidad de la información confidencial que se transmita a través de una comunicación cara a cara, por teléfono o por alguna otra vía de comunicación debe ser comunicado antes que la información sea difundida.

7.6. MANEJO Y DIFUSIÓN DE LA INFORMACIÓN CLASIFICADA

7.5.1 Aplicar los tratamientos que corresponden a cada tipo de información

- Una vez clasificada la información, se debe asignar y aplicar los tratamientos de seguridad oportunos para proteger cada tipo de información según el nivel de confidencialidad de cada una y siendo el medio en el que se presente. Podríamos establecer los siguientes tratamientos:

  - ✓ Limitar el acceso a las personas o grupos correspondientes.
  - ✓ Cifrar la información.
  - ✓ Realizar copias de seguridad.
  - ✓ Información sujeta a acuerdos de confidencialidad y no divulgación.
  - ✓ Control del acceso y/o modificación de la información.
  - ✓ Encriptación de datos.

- Todas las personas que tienen acceso a información clasificada deben de seguir lo siguiente:

	Uso Interno	Restringida	Confidencial
Documentos en Papel	- Solo las personas autorizadas pueden tener acceso. - Si es enviado fuera de la OTIN, el documento debe ser enviado por algún certificado. - Los documentos solo pueden ser guardados en lugares de acceso publico - Los documentos deben ser retirados frecuentemente de las impresoras.	- El documento debe ser almacenado en una gaveta con llave. - Los documentos pueden ser transferidos dentro y fuera de la OTIN preferentemente en un sobre cerrado. - Si es enviado fuera de la OTIN, el documento debe ser enviado con acceso de recibo. - Los documentos deben ser retirados frecuentemente de las impresoras. - Solamente el propietario del documento puede copiarlo y/o puede destruirlo.	- El documento debe ser almacenado en una caja fuerte. - El documento puede ser transferido dentro y fuera de la OTIN, únicamente por un medio confiable que garantice su confidencialidad. - No está permitido enviar el documento por correos personales. - Es posible imprimir el documento por una persona autorizada. .
Documentos Electrónicos	- Solo las personas autorizadas pueden tener acceso. - Cuando se intercambian archivos y documentos de	- Solo las personas con autorización para este documento pueden acceder a la parte del sistema de información en	- El documento debe ser almacenado en un formato encriptado. - El documento únicamente pueden ser guardado en

	la OTIN, estos deben estar protegidos con clave. - El acceso a los sistemas de información en los que están almacenados los documentos deben estar protegidos por una clave segura. - La pantalla en la que se muestra el documento debe bloquearse automáticament e luego de [cantidad] de minutos de inactividad.	el que está guardado el documento. - Cuando se intercambian archivos y documentos por FTP, estos deberán estar encriptados. - Solamente el propietario del documento puede borrarlo.	servidores confiables por la OTIN. - El documento no debe ser intercambiado a través de medios como FTP, solo por canales seguros como VPN.
Sistemas de Información	- Solo las personas autorizadas pueden tener acceso. - El acceso al sistema de información debe estar protegido por una clave segura. - La pantalla debe bloquearse automáticament e luego de cantidad] de minutos de inactividad. - El sistema de información puede estar ubicado solamente en	- Los usuarios deben finalizar la sesión en el sistema de información al abandonar temporal o permanentemen te su lugar de trabajo. - Los datos deben ser borrados solamente con un algoritmo que garantice su borrado seguro.	- El acceso al sistema de información debe estar controlado mediante un mecanismo de autenticación que utilice tarjetas inteligentes o lectores biométricos. - El sistema de información solamente puede ser ubicados en servidores controlados por la OTIN. - El sistema de información solamente

	habitaciones con acceso físico controlado.		puede estar ubicado en habitaciones con acceso físico controlados y con control de identidad de las personas.
Correo Electrónico	- Solo personas autorizadas pueden tener acceso. - El remitente debe verificar cuidadosamente el destinatario. - Aplicar todas las reglas autorizadas para "Sistemas de Información".	- El correo electrónico debe esta encriptado si se envía fuera de la OTIN.	- Todos los correos electrónicos deben ser encriptados.
Soporte de almacenamiento electrónico	- Solo las personas autorizadas podrán tener acceso. - Los soportes o archivos deben estar protegidos con clave. - Si es enviado fuera de la OTIN, el soporte debe ser enviado por correo certificado. - El soporte solo puede ser guardado en habitaciones con acceso restringido.	- Los soportes y archivos deben estar encriptados. - El soporte debe ser almacenado en un gabinete con llave. - Si es enviado fuera de la OTIN, el soporte debe ser enviado con acceso de recibo. - Solo el propietario del soporte puede tener un acceso de lectura.	- El soporte debe ser almacenado en una caja fuerte.

Información transmitida oralmente	- Solo las personas autorizadas pueden tener acceso a la información. - Las personas no autorizadas no debe estar presente en la habitación donde se comparte la información.	- La habitación debe tener restricciones de acceso. - Las conversaciones no deben ser grabados	- La conversación, mensaje, teléfono o por alguna otra vía de comunicación deben ser encriptados. - No se debe guardar ninguna transcripción de la conversación.

7.5.2 Aplicar las medidas de control de seguridad en el manejo de información

- Las medidas de de control de seguridad en el manejo de información se obtienen a través de varias fuentes. Una de las fuentes es la política de seguridad de la información de la OTIN, también otras fuentes son requisitos legales, recomendaciones de los jefes de la Unidades Funcionales y los equipos técnicos de los proyectos.

- Los colaboradores deben tener acceso a la información que le permita desempeñar sus actividades y además deben de estar comprometidos con el uso responsable de la información, siendo cada Jefe de Unidad corresponsable del buen uso que los colaboradores a su cargo hagan de la misma, por lo que es necesario tomar medidas para garantizar el cumplimiento de la presente política.

- Todos los colaboradores tienen la responsabilidad de no revelar o comunicar información **"confidencial"** o **"restringida"** a terceros. En el caso que por razones mismas del trabajo y con la autorización de su Jefe de Unidad o dentro de los parámetros permitidos en la OTIN, se bride información confidencial a terceros, se deberá firmar una Declaración de Confidencialidad (Anexo I).

- Si en el desempeño de sus actividades laborales se revela o comunica información **"confidencial"** o **"restringida"** a algún otro colaborador de la misma Oficina, es responsabilidad del colaborador a cargo de la información el advertir sobre la naturaleza de confidencialidad, dando a conocer las restricciones acerca de la difusión de dicha información.

- Los colaboradores que poseen información **"confidencial"** o **"restringida"** están prohibidos de: revelar o confiar información, hacer uso indebido y valerse directa o indirectamente, en beneficio propio o de terceros de la

información. El mal uso de dicha información puede tener consecuencias civiles o penales, sin perjuicio de la acción disciplinaria que para este caso establece la OTIN.

- Los colaboradores que culminen su vínculo laboral con la OTIN, no podrán difundir información **"confidencial"** o **"restringida"** que no haya sido publicada de manera oficial por la Institución.

7.5.3 Publicar Información

- Publicación en la página web: La página institucional (www.inei.gob.pe) es el medio de comunicación masivo de información del INEI. Busca mantener información fidedigna, veraz y actualizada. Su uso no excluye el envío físico de información cuando se considere conveniente.
  La OTIN se encarga de publicar la siguiente información:
  - ✓ Información actualizada en el Portal de Transparencia.
  - ✓ Noticias, entre otros.

- Publicación en la Intranet: La página de intranet (iinei.inei.gob.pe), es el medio de comunicación interno de la Institución, y solo se puede acceder a la información a través de un proceso de autenticación.
  La OTIN se encarga de publicar la siguiente información:
  - ✓ Información actualizada de la OTIN: Procedimientos administrativos, políticas, normas, entre otros.

- Publicación de Información vía correo electrónico.
  La OTIN se encarga de publicar la siguiente información:
  - ✓ Boletines internos de seguridad
  - ✓ Encuestas de satisfacción al usuario, entre otros.

- En el caso de información pública, su acceso constituye un derecho fundamental reconocido expresamente en la constitución (art. 2, inc. 5). "Toda persona tiene derecho a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. (...)". **Ley N° 27806.- Ley de Transparencia y Acceso a la información Pública.**

- En el caso de que la información clasificada tenga un destinatario concreto, la OTIN se tiene que asegurar que ningún tercero pueda extraer la información sin autorización.

8. CUMPLIMIENTO

- Se realizará periódicamente auditorías internas de seguridad que certifiquen que se están aplicando los tratamientos estipulados para proteger nuestra información.

9. SANCIONES

- El incumplimiento y/o violación de la presente Política que conlleve a un incidente de Seguridad de la Información ejecutado, implicará un proceso disciplinario y tendrá como resultados la aplicación de diversas sanciones y/o acciones legales, conforme a la magnitud y característica del hecho, dentro del marco legal vigente, por parte de la OTIN para establecer la responsabilidad del colaborador involucrado, independiente de la motivación.

10. ANEXOS

10.1. ANEXO I: Declaración de confidencialidad.

ANEXO I

DECLARACIÓN DE CONFIDENCIALIDAD[1]

Fecha: ...../...../.....

Por el presente documento, declaro que a toda la información recibida para realizar la ejecución de.....[Nombre del Proyecto], mediante el contrato.....[Modalidad del Contrato] de fecha inicio: ...../...../..... a fecha fin ...../...../....., le daré un tratamiento confidencial y no la revelaré a terceros.

Utilizaré toda la información recibida durante la ejecución del Contrato solamente con la finalidad especificada en el mismo.

Manejaré de forma especialmente confidencial toda la información recibida por escrito u oralmente, ya sea técnica, comercial, legal, organizacional, personal o de cualquier otro tipo, que pudiera ocasionar un daño al Instituto Nacional de Estadística e Informática – INEI si fuera divulgada a personas no autorizadas, sin importar si la información está clasificada como confidencial o no.

Solamente compartiré la información confidencial con personas que autorice el INEI en el marco del objetivo de la ejecución del Contrato.

Manejaré la información confidencial de acuerdo con lo establecido en la Ley de Protección de datos personales, Ley del Secreto Estadístico, y normas relacionadas con la seguridad de la información respetando las Políticas de Seguridad y Confidencialidad establecidas.

Si tuviera que colaborar con terceros en la ejecución del Contrato, no compartiré ningún tipo de información confidencial sin el previo consentimiento escrito del INEI.

Si fuera requerido por decisión de alguna corte jurisdiccional por un litigio, o por cualquier otro organismo judicial, gubernamental o regulador competente, o si estuviera legalmente obligado a revelar algún tipo de información confidencial, notificaré en forma inmediata y por escrito al INEI.

Si se violara alguna obligación establecida bajo esta Declaración, notificaré al INEI inmediatamente al tomar conocimiento de dicha violación.

Las obligaciones de confidencialidad bajo la presente Declaración de confidencialidad seguirán teniendo vigencia aún después del vencimiento del Contrato.

Declaro que indemnizaré al INEI por cualquier daño ocasionado por la divulgación de información confidencial.

[NOMBRES Y APELLIDOS]
N° D.N.I:.....
Oficina Técnica de informática

[1] Esta declaración debe ser firmada por todos los empleados de la organización, como también por todos los empleados de los proveedores o socios que tendrán acceso a información confidencial de acuerdo con un contrato.