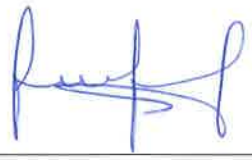
INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

OFICINA TÉCNICA DE INFORMÁTICA

POLÍTICA

"POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS DE LA OTIN"

Código: POL-002-OTIN-2018
Versión 1.0.0

POLITICA			
NOMBRE DE LA POLITICA: POLITICA DE SEGURIDAD DE LOS RECURSOS HUMANOS DE LA OTIN			
CODIGO: POL- 002 -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	**Revisado por:** Unidad Funcional de Planificación Estratégica y Gobernanza TI	**Aprobado por:** Director Técnico de la Oficina Técnica de Informática - OTIN
Nombre: Luis Taype Ignacio	**Nombre:** Jhino Arias Moreno	**Nombre:** Nelson Tucto Rodríguez	**Nombre:** Manuel Mattos Alvarado
Fecha:	**Fecha:**	**Fecha:**	**Fecha:**
Firma	**Firma**	**Firma**	**Firma**
			

Historial del Documento

Fecha de Creación:	Versión:	Modificado/Creado por:	Descripción de la modificación:
24/07/2018	1.0.0	Luis Taype Ignacio	Creación del primer documento

TABLA DE CONTENIDO

1. OBJETIVOS 4
1.1. Objetivo General 4
1.2. Objetivos Específicos 4
2. ALCANCE 4
3. MARCO LEGAL Y/O NORMATIVO 4
4. TERMINOS Y DEFINICIONES 5
5. POLITICAS 7
5.1. Política antes de desarrollar o asumir el puesto de trabajo 7
5.2. Política durante la ejecución del puesto de trabajo 8
5.3. Política de terminación del contrato o cambio del puesto de trabajo 9
6. FUNCIONES Y RESPONSABILIDADES 11
6.1. Director Técnico de la Oficina Técnica de Informática (OTIN) 11
6.2. Unidad Funcional de Planificación Estratégica y Gobernanza TI 11
6.3. Unidad Funcional de Calidad, Procesos y Seguridad de la Información 12
6.4. La Unidad Funcional de Infraestructura TIC: 12
6.5. Unidades Funcionales involucradas con la Seguridad de los activos de Información. 12
6.6. Colaboradores de la OTIN 12
7. SANCIONES 13
8. ANEXOS 14
8.1. Acuerdo de Confidencialidad 14

"POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS EN LA OTIN"

1. OBJETIVOS

1.1. Objetivo General

La presente Política tiene como objetivo incluir los criterios de seguridad de la información en la gestión de los Recursos Humanos de la Oficina Técnica de Informática – OTIN, ante un acto negligente que ponga en riesgo los activos de información de la Institución.

1.2. Objetivos Específicos

- Reducir los riesgos de error humano, comisión de ilícitos o uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.
- Dar a conocer las responsabilidades en materia de seguridad en etapa de reclutamiento y selección de los colaboradores e incluirlas en los acuerdos.
- Establecer compromisos de confidencialidad con los colaboradores y usuarios externos que tengan acceso a las instalaciones de procesamiento de información.
- Establecer mecanismos para promover la comunicación sobre las debilidades existente en materia de seguridad, así como los incidentes ocurridos, con el fin de minimizar sus efectos y prevenir su reincidencia.

2. ALCANCE

El presente documento es aplicable para los colaboradores de la OTIN, así como los usuarios externos que por motivos de las funciones que desarrolle esté en contacto con algún activo de Información.

3. MARCO LEGAL Y/O NORMATIVO

- Resolución Ministerial N° 246-2007-PCM que aprueba el uso obligatorio de la NTP ISO/IEC 17799:2007. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Ed.
- Resolución Ministerial N° 004-2016-PCM que aprueba el uso obligatorio de la NTP ISO/IEC 27001:2014
- Decreto Supremo N° 072-2012-PCM que aprueba el Código de Buenas Prácticas Estadísticas del Perú.
- Reglamento de organización y funciones (ROF), aprobado con D.S. N° 043-2001-PCM.
- Manual de Organización y Funciones (MOF), aprobado con R.J. N° 374-2004-INEI.
- Decreto Supremo Nº 056:2017-EF, que modifica el Reglamento de la Ley Nº 30225, Ley de Contrataciones del Estado.

4. TERMINOS Y DEFINICIONES

Entiéndase para efectos de la presente política, lo siguiente:

- **Activo de Información:** Todo aquello que tiene algún valor para la Institución y por lo tanto debe protegerse. Los activos de información son archivos, bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de un organización se han de considerar todos los tipos de activos de información.
- **Activo de TIC:** Los programas de cómputo, bienes informáticos, soluciones tecnológicas, sistemas o aplicativos y sus componentes, las bases de datos o archivos electrónicos.
- **Confiabilidad de la información:** La información generada debe ser adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Confidencialidad de la Información:** Característica de la información por la cual solo está disponible para personas o sistemas autorizados.
- **Cumplimiento:** Es un estado en el cual alguien o algo está de acuerdo con las directrices; las especificaciones; leyes del derecho civil y penal y los requisitos de seguridad establecidas.
- **Datos personales:** Información concerniente a una persona física, identificada o identificable, entre otras, la relativa a su origen étnico o racial, o que este referida a las características físicas, morales y emocionales, a su vida familiar, domicilio, número telefónico u otros.
- **Disponibilidad de la Información:** Característica de la información en el cual se puede garantizar que las personas autorizadas tengan acceso a la información, todas las veces que lo requiera.
- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas, electrónico, audiovisual u otro.
- **Integridad de la Información:** Característica de la información que busca mantener los datos libres de modificaciones no autorizadas.

- **Política:** Declaración de alto nivel que describe la posición de la Institución sobre un tema específico.
- **Propiedad intelectual:** Todos los productos, creaciones, desarrollos, campañas, trabajos investigaciones, etc, sujeto a explotación económica por parte de los poseedores legales de dicha propiedad.
- **Seguridad de la información:** Es el conjunto de medidas preventivas y reactivas de la Institución y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.
- **Seguridad de los Recursos Humanos:** Es el conjunto de medidas preventivas para reducir los riesgos de error humano, comisión de ilícitos contra la Institución o uso inadecuado de instalaciones.
- **Tecnologías de Información:** (**TI**, más conocida como IT por su significado en inglés, ***information technology***) es la aplicación de ordenadores y equipos de telecomunicaciones para almacenar, recuperar, transmitir y manipular datos, con frecuencia en el contexto de los negocios u otras empresas.
- **Visita:** toda persona que accede a las instalaciones de la OTIN y no mantiene un vínculo laboral directo con la Institución.

5. POLITICAS

5.1. Política antes de desarrollar o asumir el puesto de trabajo

Es necesario tener en consideración en los contratos o cualquier otra forma de vinculación laboral de los nuevos colaboradores que tendrán acceso a las instalaciones física y sistemas de información de la OTIN, lo siguiente:

Consideraciones:

- **Incorporación de Cláusulas Contractuales:** Se establecen los aspectos relevantes en relación a la seguridad de la información en la descripción de las responsabilidades de los contratos de trabajo. Se considerarán todas las responsabilidades, obligaciones y derechos legales de los colaboradores relacionado con la propiedad intelectual o la ley de protección de datos se encontrarán aclarado e incluidos en los términos y condiciones del contrato con datos de carácter personal.

- **Acuerdos de confidencialidad:** Todos los colaboradores estarán sujetos a cláusulas de confidencialidad dadas por la criticidad y sensibilidad de la información que estos manejen en la OTIN. En el caso de contratación de usuarios externos, servicios profesionales o contratos con empresas que realiza el área de logística o si el tipo de trabajo a realizar lo amerita, estos firmarán un acuerdo (**Anexo N° 1** – Acuerdo de Confidencialidad). La Unidad Funcional de Planificación Estratégica y Gobernanza TI es la encargada de hacer firmar los acuerdos de confidencialidad como corresponda.

- **Revisión de las referencias de los candidatos:** El proceso de Reclutamiento y Selección de colaboradores será canalizado a través de la Unidad Funcional de Planificación Estratégica y Gobernanza TI. En ciertas ocasiones (sobre todo para puestos de especial criticidad o con acceso a información muy confidencial) se detallarán las comprobaciones realizadas antes de incorporar un nuevo colaborador. Se determinarán los datos y referencias que han de ser revisadas en el currículum. Además, se establecerá qué puestos concretos necesitan una acreditación especial y estar libre de antecedentes penales.

  De encontrarse alguna acción irregular en el proceso de Reclutamiento y Selección, esta deberá ser reportada a la instancia que corresponde, ya sea por motivos de: si la información brindada en el currículum sea falsa, este adulterada; o de tener algún impedimento para contratar con Estado, según la Ley Nº 30225.

5.2. Política durante la ejecución del puesto de trabajo

Es necesario que los colaboradores que tengan acceso a las instalaciones físicas y sistemas de información de la OTIN, tengan en consideración lo siguiente:

Consideraciones:

- **Aceptación de las clausulas y políticas de seguridad de la información:** La Unidad Funcional de Planificación Estratégica y Gobernanza TI se asegurará que el nuevo colaborador de la OTIN lea, comprenda y firme cada uno de los acuerdos, contratos, cláusulas y documentos de políticas relacionados con la seguridad de la información.

- **Plan de formación y concienciación en materia de Seguridad de la Información:** Los colaboradores y, cuando sea pertinente los usuarios externos que desempeñen funciones en la OTIN, deberán de recibir capacitaciones de concienciación y actualización periódica en materia de Seguridad de la Información y las responsabilidades legales, así como temas referentes al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, en el ámbito de su área de trabajo y el desempeño de sus funciones . Por tal motivo se debe de aprovechar al máximo los seminarios tecnológicos que la OTIN pone a disposición a los colaboradores. De esta forma podrán comprender mejor los riesgos que enfrenta la OTIN en materia de Seguridad de la Información.

- **Concesión autorizada de los permisos de acceso:** La Unidades involucradas con la Seguridad de los activos de Información deberán garantizar que los colaboradores y, cuando sea pertinente los usuarios externos que desempeña funciones en la OTIN solo puedan acceder a los sistemas de información de manera oportuna durante las etapas del ciclo de vida de los accesos, desde el momento del registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que no requieren el acceso. Solo deberán dar de alta en los sistemas de acuerdo con las políticas de control de acceso (físico y lógico) que correspondan. En este punto, entre otras, se realiza las siguientes acciones: registro de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, recursos compartidos, autenticación de usuarios, desconexión de terminales por tiempo muerto, limitación de horario de conexión, registro de eventos, protección de puertos, subdivisión de redes, control de conexiones de red, control de ruteo, asignación de los dispositivos y equipos, etc.

- **Control de acceso a las instalaciones:** Con el fin de salvaguardar la integridad física de los sistemas de información, además de prevenir y controlar perdidas de algún activo de información, se establecerá un control obligatorio de acceso (ingreso y salida) a todos los colaboradores que desempeñen funciones dentro de las instalaciones de la Oficina Técnica de Informática - OTIN.

  La Unidad Funcional de Planificación y Gobernanza TI deberá procurar que los colaboradores desde la firma del contrato e incorporación de sus funciones en la OTIN, registren sus huellas dactilares en el lector localizado en el área de recepción de la Institución. Además, los Jefes de las Unidades Funcionales serán los responsables de constatar el cumplimiento de este mecanismo de control de acceso por parte de todos sus colaboradores.

- **Procedimientos disciplinarios:** De las sanciones a aplicar en aquellos casos en los que se haya producido una negligencia en relación con la seguridad de la información (fuga o pérdida de datos confidenciales o sensibles, actuaciones intencionadas, ataques a la reputación en redes sociales, permitir ataques de terceros como infecciones por malware, etc.) se seguirá el procedimiento disciplinario formal contemplado en el reglamento interno de la institución o lo que disponga las autoridades administrativas. Este procedimiento deberá ser notificado a todos los colaboradores y estar accesible en todo momento.

5.3. Política de terminación del contrato o cambio del puesto de trabajo

Es necesario tener en consideración del colaborador de la OTIN, que se desvincule o sea inhabilitado de sus funciones, lo siguiente:

Consideraciones:

- **Finalización del contrato:** Para evitar fugas de información es importante informar a los colaboradores las responsabilidades y obligaciones de seguridad y confidencialidad que deben cumplir una vez finalizada la relación contractual. Una vez que un colaborador deja de desempeñar funciones o prestar servicios en la OTIN, se debe informar a las entidades e instituciones externas con las que el colaborador mantenía contacto a nombre de la Institución, que éste ya no cuenta con la autorización para actuar en representación de la Institución.

  En respuesta a solicitudes de referencias de ex colaboradores de la OTIN, realizadas por entidades u organizaciones, el Jefe de la Unidad Funcional de Planificación

Estratégica y Gobernanza TI, o quien lo reemplace, será el encargado de entregar información objetiva.

- **Revocación de permisos de acceso:** Del mismo modo que en su incorporación se dieron los accesos y permisos oportunos a los nuevos colaboradores para que puedan realizar su trabajo, al finalizar la relación contractual serán revocados. Se recogerán los dispositivos entregados; se eliminarán sus cuentas de correo; se eliminarán sus permisos de acceso a sistemas y aplicativos.

6. FUNCIONES Y RESPONSABILIDADES

Para el cumplimiento de la presente Política en la OTIN, se establecen las siguientes responsabilidades a fin de que se puedan conocer, entender y asumir:

6.1. Director Técnico de la Oficina Técnica de Informática (OTIN)

- Proporcionar los recursos necesarios para garantizar la Seguridad de la Información.
- Sensibilizar a todos los colaboradores de la OTIN sobre el cumplimiento de la presente política.

6.2. Unidad Funcional de Planificación Estratégica y Gobernanza TI

- Gestionar el proceso de reclutamiento y selección de colaboradores, tanto para renovación como para nuevos contratos.
- Coordinar con la Unidad Funcional de Calidad, Procesos y Seguridad de la Información de las acciones que se van a adoptar para proteger los activos de información al interior de la OTIN.
- Incorporar cláusulas contractuales en relación a la seguridad de la Información.
- Definir los compromisos de confidencialidad para la manipulación de información crítica y sensible tanto de los colaboradores y los usuarios externos.
- Hacer firmar a los colaboradores los acuerdos de confidencialidad para las actividades de alto riesgo según la criticidad y sensibilidad de la información que estos manejen en la OTIN.
- Revisar las referencias laborales del postulante que pudieran afectar la seguridad de la información al interior de la OTIN.
- Asegurar el registro de huellas dactilares y la marcación de control de acceso de los colaboradores contratados desde el inicio de sus funciones en las instalaciones de la OTIN.
- Informar a los nuevos colaboradores sus responsabilidades y obligaciones respecto al cumplimiento de las Políticas de Seguridad de la Información definidas en la OTIN.
- Determinar los procedimientos disciplinarios que se rigen los colaboradores en el desempeño de sus funciones.
- Entregar información objetiva de ex colaboradores de la OTIN, en caso sea solicitado por entidades u organizaciones para fines laborales y/o legales.

6.3. Unidad Funcional de Calidad, Procesos y Seguridad de la Información

- Asegurar que las acciones que se adopte para proteger los activos de información se alineen a las disposiciones legales, normativas aplicables y requisitos de seguridad mencionadas en la presente política.
- Implementar medidas para reducir riesgos de error humano que comprometan la Seguridad de la Información al interior de la OTIN.
- Realizar el seguimiento, documentación y análisis de los incidentes reportados vinculado a la Seguridad de la Información.
- Difundir publicaciones de concienciación en materia de Seguridad de la Información coordinando con las Unidades Funcionales involucradas con la Seguridad de los activos de Información.
- Velar por el cumplimiento de la presente Política.

6.4. La Unidad Funcional de Infraestructura TIC:

- Gestionar adecuadamente los permisos de acceso (altas y bajas) a los activos de Información al interior de la OTIN.

6.5. Unidades Funcionales involucradas con la Seguridad de los activos de Información.

- Brindar capacitaciones/charlas, seminarios tecnológicos de concienciación en materia de Seguridad de la Información dirigido a todos los colaboradores y en especial a los que tienen acceso a los recursos, instalaciones físicas y sistemas de información al interior de la OTIN.

6.6. Colaboradores de la OTIN

- Todo colaborador, así como usuario externo tienen la obligación de cumplir con la presente Política.
- Todo colaborador deberá reportar a la Unidad Funcional de Calidad, Procesos y Seguridad de la Información – UCAPSI, con copia (cc) al Director Técnico de la OTIN, las vulnerabilidades, debilidades e incidentes de seguridad de la información que oportunamente detecten durante el cumplimiento de sus funciones.
- Ningún colaborador puede violar los sistemas computacionales y redes de la Institución, ya sea dentro o fuera del horario de trabajo.
- El personal contratado por locación de servicios está en la obligación de adjuntar el

reporte de marcación de control de acceso mensual en la parte inicial de su informe técnico (producto) como mecanismo de control de acceso a las instalaciones de la OTIN que luego será derivado al Director Técnico de la OTIN para su conformidad.

7. 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 institución para establecer la responsabilidad del colaborador involucrado, independiente de la motivación.

- DE LOS POSTULANTES, de encontrar que la información brindada en las **referencias del Curriculum** no correspondiera a los registros de las instituciones involucradas o cuya falsedad sea comprobada, se tomaran las acciones legales correspondientes; por constituir presunto delito contra la fe pública. De encontrarse que el postulante presenta impedimentos para contratar con el estado se reportarán a las autoridades administrativas o instancias que corresponde, para que se tomen las medidas establecidas según la LEY Nº 30225, como inhabilitación temporal para contratar con el Estado.

8. ANEXOS

8.1. Acuerdo de Confidencialidad

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

DECLARACIÓN DE CONFIDENCIALIDAD

Por el presente documento, declaro que a toda la información recibida para realizar la ejecución de.....[Nombre del Proyecto], mediante el contrato de .....[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 autorizadas del INEI en el marco del objetivo de la ejecución del Contrato.

Manejaré la información confidencial de acuerdo 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° DNI:.....
Oficina Técnica de Informática - OTIN