INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

## OFICINA TÉCNICA DE INFORMÁTICA

# POLÍTICAS

## "POLÍTICA DE SEGURIDAD PARA ACUERDOS CON PROVEEDORES QUE BRINDAN SERVICIOS"

**Código: POL-007-OTIN-2018**
**Versión 1.0.0**

| **POLÍTICA** | | |
|---|---|---|
| **NOMBRE DE LA POLÍTICA:** POLÍTICA DE SEGURIDAD PARA ACUERDOS CON PROVEEDORES QUE BRINDAN SERVICIOS | | |
| **CODIGO:** POL-007-OTIN-2018 | | **VERSION:** 1.0.0 |
| **PROCESO AL QUE PERTENECE:** Gestión de activos de TI | | |
| **Elaborado por:** Unidad Funcional de Calidad, Procesos y Seguridad de la Información | **Coordinado con:** Unidad Funcional de Infraestructura | **Aprobado por:** Director Técnico de la Oficina Técnica de Informática |
| **Nombre:** Ing. Katherine Montenegro Julcapoma | **Nombre:** Ing. Juan Padilla Padilla | **Nombre:** Ing. CIP Manuel Matos Alvarado |
| **Fecha:** 9/11/2018 | **Fecha:** 09/11/18 | **Fecha:** |
| **Firma** | **Firma** | **Firma** |
|  |  |  |

## TABLA DE CONTENIDO

# "POLÍTICÁ DE SEGURIDAD PARA ACUERDOS CON PROVEEDORES QUE BRINDAN SERVICIOS"

## 1. OBJETIVO

El presente documento tiene como objetivo definir las reglas básicas para la relación con proveedores de servicios en el Instituto Nacional de Estadística e Informática (INEI).

## 2. ALCANCE

La presente política se aplica a todos los proveedores de servicios que puedan tener influencia sobre la confidencialidad, integridad y disponibilidad de información sensible del INEI.

## 3. REFERENCIAS

- Norma NTP-ISO/IEC 27001:2014, capítulos A.7.1.2, A.7.2.2, A.15.1.1; A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
- Metodología para la Gestión de Riesgos de Seguridad de la Información
- Política General de Seguridad de la Información
- Política de Control de acceso

## 4. ABREVIATURAS

Las siguientes abreviaturas son aplicables para el propósito de este procedimiento:

- ✓ **OTIN:** Oficina Técnica de Informática
- ✓ **POO:** Programación Orientada a Objetos
- ✓ **SGSI:** Sistema de Gestión de Seguridad de la Información

## 5. POLÍTICA

### 5.1. INFORMACIÓN

- ✓ Toda la información que se encuentra en la red institucional, de forma escrita o circulando a través de ella mediante elementos de comunicación o transmisión, es propiedad del INEI y de carácter privado.
- ✓ La empresa proveedora de servicios asegurará que todo el personal que acceda a los Sistemas de Información del INEI o que cuente con responsabilidades en áreas de tratamiento de información, procesamiento de información, administración de sistemas y redes:

  a) Proteja los Sistemas de Información y Redes de Comunicaciones contra acceso o uso no autorizado, alteración de operaciones, destrucción, mal uso o robo.
  b) Proteja la información CONFIDENCIAL, contra divulgación no autorizada o accidental, modificación, destrucción o mal uso.

- ✓ La empresa proveedora de servicios deberá garantizar:

  a) Que la integridad, autenticación, control de acceso, auditoría y registro se contemplen e incorporen en la realización de los Proyectos y al operar los Sistemas de Información y Redes de Comunicaciones.
  b) La confidencialidad de la información almacenada tanto en formato digital como físico.

- ✓ Todos los incidentes de seguridad de la información suscitados deberán ser comunicados inmediatamente a la Dirección de la Oficina técnica de Informática (OTIN).

## 5.2. CONFIDENCIALIDAD DE LA INFORMACIÓN

- ✓ La empresa proveedora de servicios deberá asegurar que su personal guarde, por tiempo indefinido, la máxima reserva y no divulgue ni utilice directamente ni a través de terceras personas o instituciones; los datos, documentos, metodologías, claves, análisis programas y demás información a la que tengan acceso durante su relación con el INEI por la prestación de servicio de su empresa, tanto en soporte físico como digital. Esta obligación deberá continuar vigente tras la extinción del contrato laboral.
- ✓ En caso de que, por motivos relacionados directamente con el puesto de trabajo, algún trabajador de la empresa proveedora de servicios acceda a información confidencial contenida en cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.

## 5.3. CONTRATOS

- ✓ La Oficina Técnica de Informática será la encargada de proponer a la Oficina Técnica de Administración que se incluyan cláusulas de seguridad de la información de acuerdo a su competencia en los Términos de Referencia, acuerdos y contratos con proveedores. Ver Anexo 1

## 5.4. CONTROL DE ACCESO FÍSICO

- ✓ La empresa proveedora de servicios deberá garantizar que todo su personal porte su tarjeta de identificación en un lugar visible y en forma permanente.
- ✓ En casos excepcionales, por motivos de funciones, el personal de las empresas proveedoras podrá ingresar a las instalaciones del Centro de Datos bajo la vigilancia de personal autorizado del INEI y con la autorización del Director de la Oficina Técnica de Informática (OTIN), este ingreso será durante un periodo de tiempo definido.
- ✓ La unidad de Infraestructura TIC mantendrá una bitácora de ingreso de personal / visitas al Centro de datos para aquellas personas que ingresan acompañadas por el personal autorizado del INEI en donde se indicará los nombres y apellidos de la persona, la fecha, hora de ingreso y hora de salida, el nombre del personal autorizado con quien está ingresando y el motivo del ingreso firmando

## 5.5. ELIMINACIÓN DE DERECHOS DE ACCESO Y DEVOLUCIÓN DE ACTIVOS

- ✓ Una vez finalizada la relación contractual entre la empresa proveedora de servicios y el INEI, se procederá al retiro de las credenciales de acceso (usuarios, contraseñas, etc) creadas.
- ✓ La empresa proveedora de servicios tendrá la obligación de entregar los activos de propiedad del INEI empleados durante el servicio contratado.

## 6. ANEXOS

### 6.1. ANEXO 1: CLÁUSULAS DE SEGURIDAD PARA PROVEEDORES SUGERIDAS

Es necesario definir las cláusulas de Seguridad de la Información a ser incluidas en los Términos de Referencia y Contratos con proveedores, a continuación se listarán algunas sugeridas:

1. Información sobre el servicio prestado, detallar la información que se pondrá a disposición para este objetivo y cómo se clasificará.
2. Si el proveedor tiene derecho a tomar subcontratistas; si puede hacerlo, debe obtener el consentimiento escrito de parte de la Institución con un detalle de controles que deben cumplir los subcontratistas.
3. Una definición de información clasificada y cómo ser regula la protección de datos personales.
4. La duración del acuerdo y la obligación de mantener de forma confidencial y clasificada la información y/o los datos personales luego del vencimiento del contrato (al redactar este artículo, se debe tener en cuenta cómo se garantizará la continuidad del negocio en la Institución).
5. El derecho de la institución a acceder a información almacenada o procesada por el proveedor.
6. El derecho de auditar o verificar el uso de información confidencial y de controlar la ejecución del contrato en las instalaciones del proveedor, y si las auditorías pueden ser realizadas por terceros. Especificar los derechos de los auditores.
7. Las acciones requeridas luego del vencimiento del contrato (devolución, destrucción o borrado de información confidencial, devolución de equipos, etc.) para garantizar la protección de información confidencial y para asegurar la continuidad del negocio en la Institución.
8. Identificación y uso de controles clave para garantizar la protección de los activos de la Institución; por ej., controles físicos, controles para protección contra códigos maliciosos, controles de protección física, controles para proteger la integridad, disponibilidad y confidencialidad de la información, controles para asegurar la devolución o destrucción de activos de información después de ser utilizados, controles para evitar la copia y distribución de información.
9. Garantizar el acceso a informes relacionados con las actividades de negocio de los proveedores que puedan ser importantes para la Institución.
10. Responsabilidades y acciones de las partes para evitar que personas no autorizadas accedan al contrato (por ej., solamente personas que necesitan el conocimiento pueden tener derechos de acceso a la información, etc.).
11. Identificar al propietario de la información y cómo se reglamentan los derechos de propiedad intelectual y de datos personales.
12. Uso permitido de información clasificada; es decir, el método establecido para manejar ese tipo de información.
13. Proceso para notificar a la otra parte del acuerdo sobre el acceso no autorizado a la información, violaciones a la confidencialidad o cualquier otro incidente.
14. Definir el tiempo de respuesta a los incidentes y establecer un proceso de escalamiento para la resolución de problemas e incidentes.
15. Acciones resultantes por incumplimiento de contrato, responsabilidad del proveedor por transacciones y demás actividades contratadas no ejecutadas o ejecutadas a destiempo o de forma incorrecta.
16. Conocimiento del proveedor sobre políticas y procedimientos clave de la Institución.

17. Obligación de los proveedores de capacitar a los empleados para todas las actividades en las que están involucrados.
18. Comprobar que los proveedores sean conscientes de la necesidad de seguridad.
19. Prohibir que los empleados de la Institución pasen a trabajar para los proveedores.
20. Nivel de servicio deseado y nivel de servicio no aceptable.
21. Definición de los criterios de prestación de servicio, control y emisión de informes.
22. Una definición exacta del sistema y formato de informes.
23. Un proceso de gestión de cambios claramente definido.
24. Sistema de control de acceso: definir los motivos para los derechos de acceso de terceros, procesos permitidos de inicio de sesión y claves, proceso de autorización para acceso y asignación de privilegios a usuarios determinados, obligación de llevar un registro de todos los usuarios y sus derechos de acceso, procesos para eliminar derechos de acceso.
25. Una cláusula que especifique claramente que todos los derechos de acceso no autorizados explícitamente están prohibidos.
26. El derecho para supervisar y anular cualquier actividad relacionada con los activos de la Institución.
27. Controles para garantizar la continuidad del negocio de acuerdo con las prioridades de la Institución: qué servicios deben ser recuperados dentro de qué plazos.
28. Responsabilidad por daño en caso de incumplimiento de relaciones contractuales, incluyendo responsabilidad patrimonial en caso de violación de confidencialidad de la información o en caso de no prestación de servicio.
29. Responsabilidad del proveedor para almacenar datos en conformidad con las regulaciones.
30. Condiciones para prórroga o cancelación del contrato.
31. El idioma del contrato y de la comunicación futura entre la Institución y los proveedores.