



## Resolución Jefatural

Lima, 19 de SEPTIEMBRE del 2008

**VISTOS:** el Reg. 4528 (OGA) que contiene el Memorando N° 475-2008-OI-OGA/INEN de la Oficina de Informática del INEN;

**CONSIDERANDO:**

Que, mediante Decreto Supremo N° 001-2007-SA, publicado en el Diario Oficial El Peruano con fecha 11 de enero del 2007, se aprobó el Reglamento de Organización y Funciones - ROF del Organismo Público Descentralizado Instituto Nacional de Enfermedades Neoplásicas - OPD INEN;

Que, en el citado instrumento de gestión se han establecido la jurisdicción, las funciones generales y estructura orgánica del Instituto, así como las funciones de sus diferentes Unidades Orgánicas;

Que, el Inciso i) del Artículo 9° del ROF establece que es función del Jefe Institucional el aprobar, modificar y hacer cumplir documentos de gestión institucional, según las normas vigentes;

Que, mediante documento de vistos, el Director Ejecutivo de la Oficina de Informática del INEN remite la Directiva N° 01-2008-OI-OGA/INEN "Políticas Internas de Seguridad Informática del INEN" la cual tiene por finalidad definir políticas técnico administrativas de la seguridad de las tecnologías de información y comunicaciones del INEN;

Que, por los considerandos expuestos resulta necesario aprobar la citada directiva, dentro del marco de la normatividad vigente y la implementación de la OPD INEN;

Con el visto bueno del Director General de Administración del INEN;

Con las facultades conferidas por el ROF del INEN aprobado por Decreto Supremo N° 001-2007-SA;

**SE RESUELVE:**

**ARTÍCULO PRIMERO:** Aprobar Directiva N° 01-2008-OI-OGA/INEN "Políticas Internas de Seguridad Informática del INEN", la misma que en anexo adjunto forma parte integrante de la presente Resolución.

**ARTÍCULO SEGUNDO:** Encargar la difusión de la presente resolución así como su publicación en la Página Web Institucional a la Oficina de Comunicaciones.

**ARTÍCULO TERCERO:** Déjese sin efecto cualquier disposición que se oponga a la presente resolución.



**REGÍSTRESE Y COMUNÍQUESE**

Instituto Nacional de Enfermedades Neoplásicas

*[Signature]*  
Dr. Raúl Condero García-Zapata  
Jefe (e) Institucional



---

**Directiva 001- OI-OGA-INEN-2008**

**Directiva de Políticas Internas de Seguridad Informática del INEN.**

---



## INFORMACION GENERAL

### **CONTROL DOCUMENTAL:**

**PROCEDIMIENTO:** Directiva de Políticas Internas de Seguridad Informática del INEN.

**PROYECTO:** Directiva que regula las Políticas Internas de Seguridad Informática del INEN.

**ENTIDAD:** Instituto Nacional de Enfermedades Neoplásicas

**VERSIÓN:** 01

**FECHA EDICIÓN:** 10/09/2008

### **DOCUMENTOS RELACIONADOS:**

**NOMBRE DE ARCHIVO:** Directiva 01-OI-OGA- INEN-2008- PSI

### **Directiva 01-OI-INEN-2008**

**RESUMEN:** La presente directiva regula las Políticas Internas de Seguridad Informática en el Instituto Nacional de Enfermedades Neoplásicas.

### **ESTADO FORMAL:**

Preparado por:	Revisado por:	Aprobado por:
Nombre: Eduardo Corilla Baquerizo Cargo: Director Ejecutivo de la Oficina de Informática Fecha: 10 de Setiembre de 2008	Nombre: Eduardo Corilla Baquerizo Director Ejecutivo de la Oficina de Informática Fecha: 10 de Setiembre de 2008	Nombre: Eduardo Corilla Baquerizo Director Ejecutivo de la Oficina de Informática Entidad: INEN Fecha: Setiembre 2008

### **CONTROL DE VERSIONES**

FUENTE DE CAMBIO	FECHA DE SOLICITUD DEL CAMBIO	VERSIÓN	PARTES QUE CAMBIAN	DESCRIPCIÓN DEL CAMBIO	FECHA DE CAMBIO
Directiva 01-OI-OGA-INEN-2008		001	N/A		



## INDICE

Índice	03
1 Introducción	05
¿Qué son las políticas de Seguridad Informática?	06
El Instituto Nacional de Enfermedades Neoplásicas y la Seguridad Informática	06
Organización de las políticas de Seguridad Informática	07
Base Legal	07
2 Políticas Generales	08
Propietario de las políticas, normas y procedimientos de seguridad Informática.	09
Participación del personal en la Seguridad Informática	10
Sanciones al personal por faltas contra la Seguridad Informática	11
Actualización de las PSI y de las normas y/o procedimientos que las regulen	12
3 Políticas sobre Información Electrónica	12
Propietario de la información electrónica	13
Información electrónica permitida por el INEN	14
4 Políticas sobre Recursos Informáticos y Comunicaciones	15
Propietario de los Recursos Informáticos y Comunicaciones	15
Restricciones de usos de los Recursos Informáticos y Comunicaciones	16
Planes de Mantenimiento de Hardware y Aplicativos	17
5 Políticas sobre Seguridad Física	18
Seguridad de las instalaciones donde se ubican Recursos Informáticos y Comunicaciones.	18
Seguridad de los Recursos Informáticos y Comunicaciones	19
6 Políticas sobre Seguridad Lógica	20
Identificación de Recursos Informáticos y Comunicaciones	21
Identificación de Usuarios	22
Autenticación de usuarios	23
Control de acceso Internos	24
Control de accesos externos	26



7 Políticas sobre Administración de Recursos Informáticos y Comunicaciones	27
Administración de Hardware	27
Administración de Software	28
Administración de ambiente de producción	29
Administración de correo electrónico	30
Administración de copias de respaldo	31
Administración de recuperación ante contingencias	32
Administración de desarrollo de proyectos informáticos	33
Administración del mantenimiento de aplicaciones	34



## DIRECTIVA N° 001-2008-OI-OGA-INEN

### POLÍTICAS INTERNAS DE SEGURIDAD INFORMÁTICA

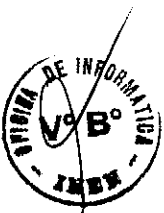
#### 1. INTRODUCCIÓN

Actualmente la seguridad informática ha tomado gran auge, dadas las cambiantes condiciones y nuevas plataformas de tecnologías de información y comunicaciones disponibles en el mercado. La Posibilidad de interconectarse a través de redes, han abierto nuevos horizontes para explorar más allá de las fronteras de nuestra organización, situación que ha llevado a ampliar la brecha de la seguridad de la información y nuevas amenazas en los sistemas de información.

Esto ha llevado a que muchas organizaciones de la administración pública y organizaciones no gubernamentales hayan desarrollado políticas, directivas y recomendaciones orientados al uso adecuado de las tecnologías de información y comunicaciones y obtener el mayor provecho de estas ventajas y evitar el uso indebido de las mismas mitigando los riesgos a los que están expuestos los sistemas de información, lo cual puede ocasionar serios problemas en los activos, bienes y servicios del INEN.

En tal sentido, las políticas de seguridad informática surgen como una herramienta para la institución, que buscan a través de las normas y/o procedimientos que las complementen, sensibilizado a cada uno de los miembros de la institución respecto a la importancia de los sistemas de información y los servicios críticos que permiten a la entidad, desarrollarse y brindar un óptimo servicio de Tecnologías de Información y Comunicaciones en beneficio de los pacientes.

Es necesario proponer e identificar una política de seguridad que requiere un alto compromiso con la institución, para establecer debilidades, y dejar constancia para renovar y actualizar dicha política en función del ambiente cambiante que rodea a las organizaciones modernas



## 1.1 ¿QUÉ SON LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA?

Las políticas de seguridad informática son un conjunto de lineamientos que establecen el marco de referencia sobre el cual se sustentan las normas y/o procedimientos, que son, en este caso, el escenario adecuado para el personal en relación con los recursos informáticos y comunicaciones y los servicios de Tecnologías de Información y Comunicaciones, enunciando lo que deseamos proteger y el por qué, sin llegar a ser una descripción técnica del mecanismo de seguridad.

Cada política de seguridad informática es una invitación de la institución a cada uno de sus miembros a reconocer la información como uno de sus **principales activos**, así como un motor de intercambio y desarrollo en el ámbito de sus funciones. Tal invitación debe concluir en una posición consciente y vigilante del personal respecto al uso y limitaciones de los recursos de Tecnologías de Información y Comunicaciones críticos de la institución.

## 1.2. EL INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS Y LA SEGURIDAD INFORMÁTICA

La Oficina de Informática del INEN ha elaborado el presente documento de Políticas de Seguridad Informática con la finalidad de asegurar la confiabilidad de las Tecnologías de Información y Comunicaciones y evitar su uso indebido, lo cual puede ocasionar serios problemas en sus bienes y servicios con respecto a las Tecnologías de Información y Comunicaciones.

El INEN considera que las políticas del presente documento por sí solas no constituyen una garantía para la seguridad informática, sino que depende principalmente del esfuerzo de todo el personal que labora en esta institución el velar por su cumplimiento.

Asimismo el INEN considera a las políticas de seguridad informática como un documento dinámico, el cual debe ser revisado y actualizado en forma periódica, dependiendo de los cambios en la institución y los avances tecnológicos de las Tecnologías de Información y Comunicaciones



## **A. ORGANIZACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA**

El presente documento está organizado en grupos de políticas, según se aprecia a continuación:

- I. Políticas Generales
- II. Políticas sobre Información Electrónica
- III. Políticas sobre Recursos Informáticos y Comunicaciones
- IV. Políticas Sobre Seguridad Física
- V. Políticas sobre Seguridad Lógica
- VI. Políticas Sobre Administración de Recursos Informáticos y Comunicaciones

En la organización de cada política se considera los siguientes aspectos:

- Objetivo
- Alcance
- Enunciado
- Responsabilidades

## **B. BASE LEGAL**

En los enunciados de las políticas del presente documento se han considerado en el marco de las siguientes normas legales que rigen para el Sector Público:

- Ley N° 28748, Ley que crea como Organismo Público Descentralizado al Instituto Nacional de Enfermedades Neoplásicas - INEN.
- Decreto Supremo N° 001-2007-SA, Reglamento de Organización y Funciones ROF del Organismo Público Descentralizado Instituto Nacional de Enfermedades Neoplásicas - OPD INEN.
- Normas de Control Interno, Resolución de Contraloría N° 320-2006-CG.





- Resolución Ministerial N° 520-2006-/MINSA, Lineamientos de Política de Seguridad de la Información.
- Norma Técnica Peruana "NTP -ISO/IEC 17799:2004 EDI. Tecnología de Información Código de Buenas Prácticas Para la Gestión de la Seguridad de la Información. 1ra Edición".-
- Resolución Directoral N° 128-DG-INEN-2006, Aprueba el Plan de seguridad de la Información y las Políticas de Seguridad de la Información.
- Modificación del capítulo X del Título V del Libro Segundo del Código Penal y que trata sobre los " Delitos Informáticos"
- Ley N° 27815, ley del Código de Ética de la Función Pública.
- Recomendaciones técnicas aprobadas por resoluciones de Jefaturas del Instituto Nacional de Estadística e Informática (INEI) que son aplicables en el INEN, de acuerdo a la potestad concedida en el Artículo 2° de su Reglamento de Organización y Funciones ( ROF) , el cual fue aprobado por el Decreto Supremo N° 043-2001-PCM
- Resolución Jefatural N° 076-95-INEI sobre "Recomendaciones Técnicas para la Seguridad e Integridad de la información que se Procesa en la Administración Pública".
- Resolución Jefatural N° 090-95-INEI, "Recomendaciones Técnicas para la Protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Pública"
- Resolución Jefatural N° 386-2002-INEI, "Normas Técnicas para el Almacenamiento y Respaldo de la Información procesada por las Entidades de la Administración Pública"

## I. POLÍTICAS GENERALES



Las Políticas consideradas en este grupo son aquellas que están relacionadas con la propiedad, conocimiento, sanciones y responsabilidades de toda

política, norma y procedimiento sobre seguridad informática emitida por la institución.

## A. PROPIETARIO DE LAS POLÍTICAS, NORMA Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA.

### Objetivo

El objetivo de esta política es definir el propietario de las políticas, normas y procedimientos de seguridad informática emitidas por el INEN, estableciendo privilegios de acceso y restricciones sobre su divulgación por parte del personal que labora en la institución.

### Alcance

El alcance de esta política involucra a todo el personal que labore en el INEN bajo cualquier modalidad, así como, a toda política, norma o procedimiento sobre la seguridad informática emitida por la organización o por dispositivos legales que rigen para la Administración Pública.

### Política

Toda política o procedimiento de seguridad informática emitida por el INEN es un documento oficial de propiedad de la organización, debiéndose establecer un grado de confidencialidad que permita asegurar su disponibilidad al personal de la institución de acuerdo a las funciones que realice.

Toda divulgación de información, política, norma o procedimiento de seguridad informática dentro de la organización debe contar con la aprobación de la Oficina de Informática y para cualquier divulgación hacia fuera de la organización debe contar con la aprobación del Jefe Institucional.

### Responsabilidad

Es responsabilidad de la Oficina de Informática el velar por el cumplimiento de estas políticas, para lo cual debe emitir normas y/o procedimientos que permitan administrar y controlar lo establecido por esta política.

Es responsabilidad de todo personal que labore en el INEN bajo cualquier modalidad el acceder exclusivamente a las políticas, normas



y procedimientos que le asigne la organización y el no divulgar a terceras personas cualquier información o documento relacionado con la seguridad informática. Estando obligado a informar a la Oficina de Informática sobre cualquier evento que afecte a esta política.

## **B. PARTICIPACIÓN DEL PERSONAL EN LA SEGURIDAD INFORMÁTICA**

### **Objetivo**

El objetivo de esta política es enmarcar la participación del personal que labora en el INEN bajo cualquier modalidad en la seguridad informática de la organización, lo cual está relacionado con el conocimiento y aplicación de las políticas, normas y procedimientos.

### **Alcance**

El alcance de esta política involucra a todo el personal que labore en el INEN bajo cualquier modalidad y a las políticas, normas o procedimientos sobre la seguridad informática emitidos por la institución.

### **Política**

Todo personal que labore en el INEN bajo cualquier modalidad es participante activo de los planes y objetivos de la Seguridad Informática de la institución por lo que deberá conocer y aplicar las políticas establecidas en el presente documento, así como los procedimientos y normas que la regulen. Con la finalidad de asegurar la integridad y confiabilidad de la información y de los recursos informáticos y comunicaciones, evitando su uso indebido, lo cual puede ocasionar riesgos que afecten a los bienes y /o servicios de Tecnologías de Información y Comunicaciones de la institución.

### **Responsabilidad**

Es responsabilidad de la Oficina de Informática el velar por el cumplimiento de esta política, para lo cual debe establecer normas y/o procedimientos que aseguren su distribución inicial y de toda actualización que se realice, así como establecer los controles necesarios que garanticen el conocimiento de los documentos mencionados de seguridad informática que la organización le otorgue.



## C. SANCIONES AL PERSONAL POR FALTAS CONTRA LA SEGURIDAD INFORMÁTICA

### Objetivo

El objetivo de esta política es establecer la existencia de sanciones al personal de la institución por faltas cometidas contra la Seguridad Informática estén contempladas o no en el presente documento.

### Alcance

Todo el personal que labore en el INEN bajo cualquier modalidad y todo riesgo que afecte la seguridad informática esté o no contemplado en dispositivos legales o en las políticas, normas y /o procedimientos de la organización.

### Política

Todo personal que labore en el INEN bajo cualquier modalidad será sancionado ante cualquier infracción contra la seguridad informática contemplada o no dentro de los artículos 207°-A, 207°-B y 207°-C del Código Penal sobre "Delitos Informáticos" o en las políticas, normas y procedimientos establecido por la institución.

Toda sanción será aplicada de acuerdo con la gravedad de la infracción y estará enmarcada dentro de los artículos 207°-A, 207°-B y 207°-C del Código Penal sobre "Delitos Informáticos". Debiendo considerar a la gravedad de la infracción por el posible riesgo ocasionado, sin ser atenuante el hecho de no haberse afectado los bienes o servicios de Tecnologías de Información y Comunicaciones de la institución.

### Responsabilidad

Es responsabilidad de la Oficina de Informática en coordinación con la Oficina General de Administración y la Oficina de Recursos Humanos establecer el grado de gravedad de las faltas y su correspondiente sanción, los cuales deberán estar indicados en las normas y/o procedimientos para cada política.

Es responsabilidad de la Oficina de Informática el velar por el cumplimiento de esta política, dar normas y/ o procedimientos para su regulación y establecer los controles con las herramientas necesarias que le permitan determinar infracciones contra la seguridad informática.



Es responsabilidad de la Oficina General de Administración y la Oficina de Recursos Humanos el aplicar, informar y registrar toda infracción cometida con la seguridad informática.

#### **D. ACTUALIZACIÓN DE LAS POLÍTICAS DE LA SEGURIDAD INFORMÁTICA Y DE LAS NORMAS Y/O PROCEDIMIENTOS QUE LAS REGULEN.**

##### **Objetivo**

El objetivo de esta política es definir el ente encargado de actualizar las políticas de Seguridad Informática de la institución, así como de toda norma y/ o procedimiento que regulen a dichas políticas

##### **Alcance**

Toda modificación que se deba realizar a las políticas de Seguridad Informática y a las normas y/o procedimientos que la regulen. Considerando como modificación las acciones de añadir, cambiar o eliminar parte o totalidad de los documentos.

##### **Política**

La función de administrar, controlar y actualizar el presente documento, así como de establecer las normas y/o procedimientos que regulen cada política es de la Oficina de Informática. Siendo de vital importancia el realizar esta función en forma correcta y oportuna, de tal forma que permita garantizar la integridad y confiabilidad de los servicios informáticos.

##### **Responsabilidad**

Es responsabilidad de la Oficina de Informática el administrar, controlar y actualizar el presente documento, así como establecer las normas y procedimientos que permitan cumplir en forma correcta con lo establecido por esta política.

## **II. POLÍTICAS SOBRE INFORMACIÓN ELECTRÓNICA**

Las políticas consideradas en este grupo son aquellas que están relacionadas con la propiedad, restricción y protección de la información electrónica de la institución.



## A. PROPIETARIO DE LA INFORMACIÓN ELECTRÓNICA

### Objetivo

El objetivo de esta política es establecer la propiedad de la información electrónica por parte de la institución, así como las restricciones sobre su utilización o divulgación de acuerdo a lo dispuesto por la institución, a dispositivos legales aplicables y a las recomendaciones técnicas del INEI y la ONGEI.

### Alcance

De acuerdo con la definición de información electrónica, el alcance de esta política es toda información que se almacene o se procese o se acceda en cualquier activo informático de la organización.

### Política

El INEN es propietario único y exclusivo de toda información electrónica de la institución, la cual dependiendo de su tipo y grado de sensibilidad, debe ser identificado, controlado y protegido. Por tal motivo todo acceso a la información electrónica dentro de la organización debe ser autorizado, identificado y controlado por el área correspondiente de su custodia.

Toda divulgación de la información electrónica hacia afuera de la organización debe contar con la aprobación del Jefe Institucional del INEN.

Toda utilización, ingreso o interferencia indebida sobre información electrónica de la organización será considerado como "Delitos Informáticos", de acuerdo al artículo 207° B y 207° C del Código Penal.

Las normas y/o procedimientos que regulen esta política deben de estar alineadas con lo establecido por el INEI en una Resolución Jefatural N° 076-95-INEI sobre "Recomendaciones Técnicas para la Seguridad e Integridad de la información que se Procesa en la Administración Pública".

### Responsabilidad

Es responsabilidad de la Oficina de Informática administrar y custodiar la información electrónica del INEN, estableciendo normas y/o procedimientos que aseguren la integridad, confidencialidad y propiedad



de la información, para lo cual debe establecer controles con las herramientas necesarias que garanticen el cumplimiento de esta política

Es responsabilidad de todo el personal que labore en el INEN el velar por el cumplimiento de esta política, de las normas y/o procedimientos que la regulen. Asimismo, está obligado a informar a la Oficina de Informática sobre cualquier divulgación o uso indebido de la información electrónica.

## **B. INFORMACIÓN ELECTRÓNICA PERMITIDA POR EL INEN.**

### **Objetivo**

El objetivo de esta política es definir la información electrónica a la cual, El INEN permite acceder o almacenar en sus recursos informáticos y comunicaciones.

### **Alcance**

De acuerdo con la definición de información electrónica, el alcance de esta política es toda información que se almacene o se procese o se acceda en cualquier activo informático de propiedad o en alquiler que presten servicios al INEN.

### **Política**

El personal que labore en el INEN bajo cualquier modalidad sólo podrá acceder, procesar o almacenar información electrónica que esté de acuerdo con sus funciones asignadas.

Por tal motivo está prohibido que el personal en mención tenga en los recursos informáticos y comunicaciones de la institución, información que no compete a sus labores. El personal de informática está facultado de informar sobre estos hechos, sin necesidad de avisar o solicitar permiso de los usuarios.

### **Responsabilidad**

Es responsabilidad de la Oficina de Informática, dar normas y /o procedimientos que regulen esta política y de establecer controles con las herramientas necesarias para verificar que en los recursos informáticos de la institución, sólo exista información que corresponda a las funciones del INEN y que corresponda a las labores desempeñadas por cada persona.

Es responsabilidad de todo el personal que labore en el INEN el velar por el cumplimiento de esta política, de sus normas y/o procedimientos que



la regulen. Asimismo está obligado a informar a la Oficina de Informática, de toda información que se encuentra en los activos informáticos de la organización y que sea ajena a las funciones del INEN.

### III. POLÍTICA SOBRE RECURSOS INFORMÁTICOS Y COMUNICACIONES

Las políticas consideradas están relacionadas con la propiedad de los recursos informáticos y comunicaciones las restricciones sobre su uso. A fin de garantizar su integridad y su correcto empleo.

#### A. PROPIEDAD DE LOS RECURSOS INFORMÁTICOS Y COMUNICACIONES

##### Objetivo

El objetivo de esta política es establecer la propiedad de los recursos informáticos y comunicaciones adquiridos que presten servicios al INEN, así como establecer las restricciones sobre su utilización.

##### Alcance

De acuerdo con la definición de recursos informáticos y comunicaciones, el alcance de esta política es todo recurso informático y comunicación que tenga relación con el almacenar, procesar, acceder a la información electrónica y la transmisión de datos de la institución, que sea de propiedad del INEN. Queda excluida de esta política todo programa o software que esté licenciado por uso.

##### Política

El INEN es propietario único y exclusivo de todos los recursos informáticos y comunicaciones adquiridas que le presten servicios a la organización, siempre y cuando no se traten de programas o software licenciado en uso.

Tratándose de recursos informáticos y comunicación alquilados por el INEN que le presten servicios, el INEN se reserva todos los derechos derivados de su uso.

Todo recurso informático y comunicación que sea adquirido por el INEN debe ser asignado, administrado, controlado y baja por la Oficina de Informática, a fin de garantizar su integridad



Toda asignación de recursos informáticos y comunicaciones del INEN asignado a personal que no labore en la organización deberá estar debidamente autorizada por el Jefe de Institucional.

### **Responsabilidad**

Es responsabilidad de la Oficina de Informática administrar, asignar, mantener controlar, dar de baja y emitir informe técnico de todo los recursos informáticos y comunicaciones que exista en la organización, emitir normas y/o procedimientos que regulen y establecer controles con las herramientas necesarias que garanticen su cumplimiento.

Es responsabilidad de todo el personal que labore en el INEN el custodiar los recursos informáticos y comunicaciones que se le asignen, el velar por el cumplimiento de esta política y las normas y/o procedimientos que la regulen. Asimismo está obligado a informar a la Oficina de Informática sobre cualquier evento que ponga en riesgo los recursos informáticos y comunicaciones que existan en la organización.

## **B. RESTRICCIONES DE USO DE LOS RECURSOS INFORMÁTICOS Y COMUNICACIONES**

### **Objetivo**

El objetivo de esta política es establecer las restricciones de uso de los recursos informáticos y comunicaciones que existan en la organización, a fin de evitar usos indebidos o eventos que pongan en riesgo dichos recursos.

### **Alcance**

De acuerdo con la definición de recursos informáticos y comunicaciones, el alcance de esta política es todo medio que tenga relación con el almacenar, procesar o acceder a la información, que sea de propiedad o esté en alquiler por la organización.

### **Política**

El personal que labore en el INEN bajo cualquier modalidad esta prohibido de emplear los recursos informáticos y comunicaciones existentes en la organización para fines comerciales o de carácter personal que sean ajenos a las funciones del INEN. Por tal motivo la Oficina de Informática del INEN puede con justificación y aprobación debida, revisar, monitorear o



registrar cualquier recurso informático y comunicación sin previo aviso o permiso del usuario

Toda utilización, ingreso o interferencia indebida sobre recursos informáticos y comunicaciones existentes en la organización será considerado "Delitos Informáticos", de acuerdo a los artículos 270°-A, 207°-B y 207°-C del Código Penal.

### **Responsabilidad**

Es responsabilidad de la Oficina de Informática velar por el cumplimiento de esta política, dar normas y/ procedimientos que la regulen y establecer controles con las herramientas necesarias que le permitan verificar el empleo de los recursos informáticos y comunicaciones en funciones propias de la organización.

Es responsabilidad de todo el personal que labore en el INEN el velar por el cumplimiento de esta política, de sus normas y/o procedimientos que la regulen. Asimismo esta obligado, a informar a la Oficina de Informática de todo recurso informático y comunicación en el que se realicen labores ajenas a las funciones de la organización.

## **C. PLANES DE MANTENIMIENTO DE HARDWARE Y APLICATIVOS**

### **Objetivo**

El objetivo de esta política es de dar lineamientos para el mantenimiento de recursos informáticos y comunicaciones y aplicativos, con la finalidad de proteger y garantizar su correcto funcionamiento de los recursos informáticos y los sistemas de información.

### **Alcance**

Comprende a todos los recursos informáticos y comunicaciones y aplicativos, de todas las áreas o personal de la institución que tienen responsabilidad sobre ellos o que de alguna forma tiene relación directa o indirecta.

### **Política**

La Oficina de Informática es la encargada de la elaboración de planes de mantenimiento preventivo y correctivo de los recursos informáticos y comunicaciones (hardware) y aplicativos, conservación de sus instalaciones y ejecución de dichos planes, salvo excepciones de



mantenimiento que están fuera de su alcance o no corresponden a su materia.

#### **IV. POLÍTICAS SOBRE SEGURIDAD FÍSICA**

Estas políticas buscan proteger los recursos informáticos y comunicaciones de riesgos físicos que afecten su correcto funcionamiento. Esta protección está enfocada a prevenir amenazas causadas por lugares inadecuados para el funcionamiento de los recursos informáticos y comunicaciones, así como la protección física de los mismos recursos.

##### **A. SEGURIDAD DE LAS INSTALACIONES DONDE SE UBICAN LOS RECURSOS INFORMÁTICOS Y COMUNICACIONES**

###### **Objetivo**

El objetivo de esta política es definir las condiciones de seguridad de los lugares en donde se instalen recursos informáticos y comunicaciones.

###### **Alcance**

Comprende a los lugares donde se instalen recursos informáticos y comunicaciones al personal encargado de las instalaciones.

###### **Política**

Todo lugar donde se instalen o se almacenen recursos informáticos y comunicaciones debe contar con las medidas de seguridad necesarias y cumplir con los requerimientos técnicos especializados por el proveedor de recurso, a fin de garantizar su integridad.

Todo lugar donde se instale algún recurso informático y de comunicación deberá ser aprobado por la Oficina de Informática. Para lo cual, antes de instalar algún recurso informático y de comunicación en alguna área, se deberá verificar el cumplimiento de los requerimientos necesarios de lugar, tales como: ubicación, condiciones ambientales, suministros de energía, pozos a tierra, elementos de comunicación, requerimientos técnicos especializados por el proveedor del recurso, mantenimiento adecuado (limpieza y orden) y seguridad contra acceso físico, inundaciones e incendios.



Toda instalación de los recursos es función exclusiva de la Oficina de Informática. Por tal motivo está prohibida la instalación de recursos informáticos y comunicaciones por personal no autorizado por dicha Oficina.

Las normas y los procedimientos que regulen esta política deben de estar alineados con lo establecido por el INEI en su Resolución Jefatural N° 009-95-INEI sobre "Recomendaciones Técnicas para la protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Pública".

### **Responsabilidad**

Es responsabilidad de la Oficina de Informática el velar por el cumplimiento de esta política, dar las normas y/o procedimientos que la regulen y establecer controles con las herramientas necesarias que garanticen la seguridad física de los recursos informáticos y comunicaciones.

Es responsabilidad de todo el personal que labore en el INEN bajo cualquier modalidad, el cumplir con esta política, las normas y/o procedimientos que la regulen. Asimismo está obligado a informar a la Oficina de Informática sobre cualquier instalación de algún recurso informático y de comunicación que sea realizada por personal no autorizado y/o en lugares no autorizados.

## **B. SEGURIDAD DE LOS RECURSOS INFORMÁTICOS Y COMUNICACIONES**

### **Objetivo**

El objetivo de esta política es establecer las medidas necesarias de seguridad física sobre los recursos informáticos y comunicaciones, con relación a la manipulación por personal no autorizado, cambios, robos totales o parciales de sus partes o cualquier evento que ponga en riesgo su correcto funcionamiento.

### **Alcance**

El alcance de esta política es todo recurso informático y de comunicación que sea de propiedad o esté alquilado por la institución, así como a todo personal que esté encargado de su manipulación.



### Política

Todo recurso informático y de comunicación debe contar con las medidas necesarias de seguridad física a fin de evitar riesgos contra manipulaciones indebidas, cambios de sus partes, robos parciales o totales. Tales medidas pueden ser cerraduras contra desembalaje, seguros para computadoras portátiles, de fluido electrónico, cajas con llave para almacenar medios de respaldo. etc.

Todo servicio técnico a los recursos informáticos y comunicaciones debe ser realizado únicamente por personal autorizado de la Oficina de Informática.

Toda norma y/o procedimiento que regulen esta política debe de estar alineada con lo establecido por el INEI en su Resolución Jefatural N° 090-95 -INEI sobre: "Recomendaciones Técnicas para la Protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Pública".

### Responsabilidad

Es responsabilidad de la Oficina de Informática velar por el cumplimiento de esta política, de dar normas y/o procedimientos que regulen y establecer controles que garanticen su cumplimiento.

Es responsabilidad de todo el personal que labore en el INEN, el velar por el cumplimiento de esta política, de sus normas y /o procedimientos que la regulen. Asimismo está obligado a informar a la Oficina de Informática sobre cualquier evento que pueda afectar a la seguridad física o manipulación inadecuada de los recursos informáticos y comunicaciones.

## **V. POLÍTICAS SOBRE SEGURIDAD LÓGICA**

Las políticas sobre seguridad lógica buscan identificar, establecer, controlar y administrar los privilegios de acceso a la información electrónica de los usuarios de acuerdo a las funciones que le ha asignado la organización, de forma tal que se garantice que toda información sea accedida y modificada por personal autorizado.



## A. IDENTIFICACIÓN DE RECURSOS INFORMÁTICOS Y COMUNICACIONES

### Objetivo

El objetivo de esta política es identificar en forma electrónica los componentes de la red informática que participan en el intercambio de información, con la finalidad de garantizar la óptima transmisión de datos.

### Alcance

El alcance de esta política es para todo recurso informático y de comunicación que participe en el intercambio de información en la red informática, tales como servidores, computadoras, equipos de comunicación (concentradores switch, módem, centrales telefónicas, impresoras, etc.).

### Política

Todo recurso informático que participe en forma directa en el intercambio de información de la red debe tener una identificación o dirección electrónica única, con la finalidad de garantizar el correcto tráfico de la información en la red.

Toda identificación a los recursos informáticos y comunicaciones que estén relacionados con el intercambio de información en la red, debe ser asignado, modificado y controlado por personal autorizado de la Oficina de Informática. Por tal motivo está prohibido que personal no autorizado por dicha oficina realice cualquier asignación o cambio de identificación de los recursos informáticos y comunicaciones.

### Responsabilidad

Es responsabilidad de la Oficina de Informática el velar por el cumplimiento de esta política, dar normas y/o procedimientos que la regulen y establecer controles con las herramientas necesarias que le permitan garantizar el correcto intercambio de información entre los recursos informáticos y comunicaciones.

Es responsabilidad de todo el personal que labore en el INEN, bajo cualquier modalidad, el velar por el cumplimiento de esta política, de sus normas y/o procedimientos que la regulen. Debiendo informar a la Oficina de Informática, de toda modificación de la identificación de los



recursos informáticos y comunicaciones realizado por personal no autorizado.

## B. IDENTIFICACIÓN DE USUARIOS.

### Objeto

El objetivo de esta política es identificar en forma unívoca a cada usuario que utilice los Sistemas de Información, con la finalidad de otorgarle accesos a la información electrónica y a los recursos informáticos y comunicaciones de la organización. Esta identificación se relaciona con los privilegios otorgados a cada usuario en función a las labores que desempeña.

### Alcance

El alcance de esta política es para todo usuario que acceda a la información electrónica mediante el uso de la red, sistemas, aplicaciones y servidores, en forma interna o externa.

### Política

Toda persona que labore en la organización, bajo cualquier modalidad, de acuerdo a sus funciones asignadas en la organización, que deba acceder a la información electrónica, lo hará mediante un identificador de usuario (Userid)

Todo identificador de usuario deberá ser único, de carácter personal, intransferible y de uso obligatorio para los fines otorgados. Dado a que el identificador establece una relación entre las funciones asignadas al usuario y los privilegios de acceso a la información electrónica de propiedad del INEN.

Toda administración y control de los identificadores de usuario y de los privilegios otorgado de acceso a la información electrónica de la organización es función de la Oficina de Informática.

Todo uso indebido de los identificadores de usuario o de los privilegios de acceso otorgados por la organización, son considerados "Delitos Informáticos", de acuerdo al Decreto Ley N° 635 del Código Penal, capítulo 10 del Título V del libro Segundo.



Toda norma y/o procedimiento que regule esta política debe estar alineada con lo establecido por el INEI en su Resolución Jefatural N° 076-95-INEI sobre "Recomendaciones Técnicas para la Seguridad e Integridad de la información que se Procesa en la Administración Pública".

### **Responsabilidad**

Es responsabilidad de la Oficina de Informática velar por el cumplimiento de esta política, de dar las normas y/o procedimientos que la regulen y establecer controles con las herramientas necesarias que garanticen su cumplimiento.

Es responsabilidad de todo el personal que labore en el INEN el utilizar únicamente la(s) identificación(es) de usuario que le han sido otorgada(s). Siendo de su total responsabilidad el empleo de ellas(os) por terceras personas. Asimismo es de su obligación, informar a la Oficina de Informática de cualquier empleo indebido de identificación de usuarios.

## **C. AUTENTIFICACIÓN DE USUARIOS**

### **Objetivo**

El objetivo de esta política es definir el derecho de autenticar que el usuario es realmente la persona que argumenta ser, para lo cual el usuario ratifica su identidad suministrando una clave o contraseña que sólo él conoce. Teniendo como finalidad el garantizar que todo acceso a la información electrónica realizada mediante un identificador de usuarios pertenece a dicho usuario.

### **Alcance**

La autenticidad del usuario está relacionada en forma directa con la identificación del usuario, por tal motivo el alcance de esta política es para toda identificación del usuario otorgada.

### **Política**

Todo personal de la organización que se le haya asignado una identificación de usuario tiene el derecho y la obligación de usar su contraseña personal, exclusiva y confidencial. Por tal motivo se considera que todo acceso o alteración de información electrónica efectuada con una identificación de usuario es realizado por dicho usuario.





Toda contraseña definida por los usuarios de los servicios de los Sistemas de Información deberá respetar las normas establecidas para su generación. Siendo función de la Oficina de Informática el emitir dichas normas, las cuales deberán estar alineadas con lo establecido por el INEI en su Resolución Jefatural N° 076-95-INEI sobre "Recomendaciones Técnicas para la Seguridad e Integridad de la Información que se Procesa en la Administración Pública".

### Responsabilidad

Es responsabilidad de la Oficina de Informática establecer normas y/o procedimientos que regulen esta política, así como establecer los controles con las herramientas necesarias para garantizar la confidencialidad de las contraseñas.

Es responsabilidad de todo usuario mantener la confidencialidad de su contraseña, asimismo es de su total responsabilidad los accesos o alteraciones de información realizada con su identificación de usuario. También es responsabilidad del usuario el velar por el cumplimiento de esta política, de las normas y/o procedimientos que la regulen, estando obligado a informar a la Oficina de Informática de cualquier evento que afecte la confidencialidad de las contraseñas.

## **D. CONTROL DE ACCESOS INTERNOS.**

### Objetivo

El objetivo de esta política es definir la asignación de privilegios para el acceso a la información electrónica, de acuerdo a las funciones del personal que labora en el INEN, de igual forma, definir los accesos a recursos informáticos y comunicaciones de la institución, con la finalidad de minimizar el riesgo por accesos no autorizados.

### Alcance

A toda aplicación administrativa y asistencial que utilice la organización para el cumplimiento de sus funciones, tales como Sistema Integrado de Gestión Administrativa SIGA y Sistema Integrado Hospitalario SYSINEN.

### Política

Los Directores y Jefes de Oficinas, Departamentos y/o Servicios del INEN son los dueños de la información electrónica de los sistemas que



están relacionados directamente con la gestión de sus funciones. Por tal motivo son los que establecen los privilegios de acceso a su información y autorizan la asignación de dichos privilegios al personal de la organización, de acuerdo a sus funciones asignadas.

La Oficina de Informática tiene la función de administrar, asignar y custodiar los privilegios de acceso a la información de la institución.

La Oficina de Informática es el único ente que puede autorizar y designar el empleo de técnicas y/o herramientas que sirvan para encontrar debilidades de seguridad de acceso a los servicios informáticos de la institución (hacking ético). Por tal motivo sin la autorización debida de esta Oficina, está prohibido que el personal que labore en el INEN bajo cualquier modalidad utilice o pruebe cualquier técnica y/o herramienta que viole o busque encontrar debilidades en la seguridad de accesos a servicios informáticos desde o hacia la institución.

Todo acceso no autorizado a los servicios informáticos de la institución es considerado "Delito Informático", de acuerdo a los artículos 207°-A, 207°-B y 207°-C del Código Penal.

### **Responsabilidad**

Es responsabilidad exclusiva de cada Director y Jefe de Oficina, Departamento y/o Servicio del INEN, el definir los privilegios de acceso a la información de su propiedad y autorizar la asignación de dichos privilegios al personal de la institución.

Es responsabilidad de la Oficina de Informática establecer normas y/o procedimientos que regulen esta política, así como de establecer los controles con las herramientas necesarias para verificar el cumplimiento de esta política y de sus normas y/o procedimientos que la regulen.

Es responsabilidad de todo personal que labore en el INEN el velar por el cumplimiento de esta política, de sus normas y/o procedimientos que la regulen, asimismo es de su obligación, informar a la Oficina de Informática de cualquier empleo de técnicas y/o herramientas que sirvan para encontrar debilidades de seguridad de acceso a los Sistemas de Información.



## E. CONTROL DE ACCESOS EXTERNOS

### Objetivo

El objetivo de esta política es minimizar el riesgo por accesos de terceras personas (intrusos) o por virus que provenga de redes externas a la de la institución, mediante el empleo de herramientas de seguridad o restricciones operativas. La finalidad de control de acceso externo es garantizar la integridad de la información electrónica y los recursos informáticos y comunicaciones.

### Alcance

Todo recurso que permita el acceso externo de intrusos a los Sistemas de Información de la institución, así como todo recurso que permita evitarlo.

### Política

La Oficina de Informática está encargada de la seguridad sobre el control de accesos externos a los Sistemas de Información, por lo cual es la única que puede autorizar, instalar y configurar los equipos que tengan este privilegio.

Todo acceso no autorizado a los Sistemas de Información de la organización es considerado "Delito Informático" de acuerdo a los artículos 207-A, 207-B, 207-C del Código Penal.

### Responsabilidad

Es responsabilidad de la Oficina de Informática establecer normas y/o procedimiento que regulen esta política, así como de establecer los controles con las herramientas necesarias para el cumplimiento de esta política y de sus normas y /o procedimientos que la regulen.

Es responsabilidad de todo el personal que labore en el INEN el velar por el cumplimiento de esta política, de sus normas y/o procedimientos que la regulen. Asimismo es de su obligación, informar a la Oficina de Informática de cualquier evento que afecta la seguridad sobre el control de accesos externos a los Sistemas de Información de la organización.



## VI. POLÍTICAS SOBRE ADMINISTRACIÓN DE RECURSOS INFOMATICOS Y COMUNICACIONES

### A. ADMINISTRACIÓN DE HARDWARE

#### Objetivo

El objetivo de esta política es de dar lineamientos para la administración del Hardware o recursos informáticos y comunicaciones, con la finalidad de proteger su integridad y garantizar su funcionalidad.

#### Alcance

Comprende a todos los recursos informáticos y comunicaciones, a toda área o personal de la institución que tienen responsabilidad sobre ellos o que de alguna forma tiene relación directa o indirecta.

#### Política

La Oficina de Informática es el ente encargado de administrar los recursos informáticos y comunicaciones de propiedad o alquiler de la institución, para lo cual debe realizar actividades como el registro, traslado, instalación, asignación, mantenimiento, configuración y custodia de los recursos informáticos y comunicaciones de propiedad de la institución.

Está prohibido que personal no autorizado por la Oficina de Informática realice alguna actividad de traslado o instalación o mantenimiento o configuración de los recursos informáticos y comunicaciones, siendo excepciones a esta prohibición el traslado de los equipos portátiles y la custodia de equipos informáticos que estén asignados a usuarios.

La Oficina de Informática, también está encargada de aprobar los requerimientos, la evaluación de las propuestas de los proveedores, la recepción y los servicios, que estén relacionados en forma directa o indirecta con los recursos informáticos y comunicaciones de la institución

#### Responsabilidad

Es responsabilidad de la Oficina de Informática la administración de recursos informáticos y comunicaciones de la institución y debe participar de todo proceso de adquisición o alquiler o contrato de servicios relacionados con recursos informáticos y comunicaciones del INEN para lo cual debe dar normas y/o procedimientos que regulen



esta política y establecer controles que le permitan verificar el cumplimiento de esta política.

Es responsabilidad de la Oficina de Logística el informar a la Oficina de Informática sobre todo proceso de adquisición, alquiler, recepción, evaluación de propuestas de proveedores de recursos informáticos y comunicaciones y de servicios contratados que tengan relación directa o indirecta con los recursos informáticos y comunicaciones de la institución.

## **B. ADMINISTRACIÓN DE SOFTWARE**

### **Objetivo**

El objetivo de esta política es dar lineamientos para la correcta administración del software, respetando los derechos de autor y la propiedad intelectual, con la finalidad de proteger su integridad y garantizar su funcionalidad.

### **Alcance**

Comprende a todo software desarrollado o licenciado en uso por la institución, así como a todas las áreas o personal de la organización que tengan responsabilidad sobre ellos.

### **Política**

La Oficina de Informática es el ente encargado de la administración de software, para lo cual realiza acciones, de registro, instalación, actualización y configuración del mismo en los recursos informáticos y comunicaciones de la organización, respetando los derechos de autor, el número de licencias y la propiedad intelectual del software.

Está prohibido que personal no autorizado por la Oficina de Informática, realice alguna actividad de instalación o actualización o configuración de software en los recursos informáticos y comunicaciones de la organización. En la categoría del Software no autorizados por la institución se incluyen programas tales como: juegos, reproductores de música, protectores de pantalla, aplicativos particulares, aplicativos recibidos por la red a través de Internet, aplicativos entregados en calidad de prueba (aplicativos en demostración o autorizaciones por un lapso o número de procesos) empaquetadores, etc.



La Oficina de Informática también está encargada de aprobar los requerimientos, la evaluación de las propuestas de los proveedores, la recepción y los servicios, que estén relacionados en forma directa o indirectamente con el software de la institución.

### **Responsabilidad**

Es responsabilidad de la Oficina de Informática la administración del software de la organización y debe participar de todo proceso de adquisición o alquiler o contrato de servicios relacionados al software del INEN, para lo cual debe dar normas y/o procedimientos que regulen esta política y establecer controles que le permitan verificar su cumplimiento.

Es responsabilidad de la Oficina de Logística el informar a la Oficina de Informática sobre todo el proceso de adquisición, alquiler, recepción, evaluación de propuestas de los proveedores de software y de servicios contratados que tengan relación directa o indirecta con el software de la institución.

Es responsabilidad de todo usuario cumplir con esta política y sus normas y/o procedimientos que la regulen. Asimismo está obligado a informar a la Oficina de Informática cualquier evento que afecte la administración del software de la institución.

## **C. ADMINISTRACIÓN DE AMBIENTE DE PRODUCCIÓN.**

### **Objetivo**

El objetivo de esta política, es aumentar la confiabilidad de los procesos ejecutados en el ambiente de producción, a fin de garantizar la calidad y continuidad del servicio.

### **Alcance**

Comprende a todo recurso centralizado, utilizado para procesos ejecutados en ambiente de producción.

### **Política**

La Oficina de Informática es el ente encargado del ambiente de producción, para lo cual debe establecer actividades que garanticen su integridad, funcionamiento y servicio a la organización. Estas



actividades están relacionadas con la administración y custodia de los recursos centralizados, tales como: administración de procesos, de redes y telecomunicaciones, de correo electrónico, de pases a producción de desarrollos y cambios en los sistemas, planes de respaldo, planes de recuperación y otras actividades asignadas de acuerdo al manual de organización y funciones.

### **Responsabilidad**

Es responsabilidad de la Oficina de Informática establecer normas y/o procedimientos que regulen esta política, así como de establecer los controles con las herramientas necesarias para el cumplimiento de esta política y de sus normas y/o procedimientos que la regulen.

Es responsabilidad de todo usuario cumplir con esta política y sus normas y/o procedimientos que la regulen. Asimismo está obligado a informar a la Oficina de Informática cualquier evento que afecte la administración del ambiente de producción

## **D. ADMINISTRACIÓN DEL CORREO ELECTRÓNICO.**

### **Objetivo**

El objetivo de esta política es permitir una rápida y eficiente comunicación, basada en la utilización apropiada del servicio de correo electrónico y en propósitos relacionados con las funciones de la institución.

### **Alcance**

Comprende a todo personal que labore en la institución bajo cualquier modalidad, que tenga cuenta de correo electrónico de la organización.

### **Política**

La Oficina de Informática es el ente encargado de la administración del correo electrónico, para lo cual debe asegurar su operación continua, mantener actualizado las cuentas, tomar medidas de seguridad contra virus y controlar el uso debido del correo por parte de los usuarios.

El INEN considera los correos electrónicos como información electrónica de su propiedad y que son considerados documentos oficiales para todo uso. Por tal motivo se prohíbe a todo el personal que labore en la institución bajo cualquier modalidad: el uso de cuentas de correo que no



le han sido otorgado, el empleo del correo para uso personal o de negocios ajenos a sus funciones, el uso de lenguaje obsceno y/o abusivo.

### Responsabilidad

Es responsabilidad de la Oficina de Informática de administrar el correo electrónico, mediante normas y/o procedimientos que regulan esta política y establecer controles con las herramientas necesarias que le permitan verificar el cumplimiento de esta política.

Es responsabilidad de todo usuario cumplir con esta política y sus normas y/o procedimientos que la regulen. Asimismo está obligado a informar a la Oficina de Informática cualquier evento que afecte la administración del correo electrónico.

## E. ADMINISTRACIÓN DE COPIAS DE RESPALDO

### Objetivo

El objetivo de esta política es salvaguardar la integridad de los datos y software en general, mediante el empleo de copias de respaldo, que permitan garantizar la continuidad de las operaciones de los sistemas de información ante la eventual presencia de fallas o contingencias.

### Alcance

Toda información sensible y necesaria para la continuidad de los sistemas de información. Esta información sensible constituida por la información electrónica de propiedad del INEN y de los recursos del software que incluye a: software en general, sistemas operativos, sistemas aplicaciones, correos y otros.

### Política

La Oficina de Informática es el ente encargado de la administración de las copias de respaldo concerniente a la información sensible de la organización y que residan en recursos compartidos de la red. Para el desarrollo de esta función debe realizar estudios sobre la información sensible, tales como: identificación, que tan crítico resulta para la organización, que tanto cambia en el tiempo, volumen de información y otros. Con estas actividades determina la importancia de la información, la periodicidad, tiempo de retención y cantidad de las copias de respaldo.





La Oficina de Informática debe verificar que las copias de respaldo cumplen su cometido, para lo cual debe realizar pruebas de recuperación de la información sensible, a fin de garantizar que los procesos y los medios de respaldo funcionan correctamente.

Todo personal que labore en el INEN bajo cualquier modalidad no debe almacenar información sensible de la organización en los discos duros de las computadoras personales o portátiles, porque de ocurrir una falta de disco o el robo del equipo significaría pérdidas para la institución.

Toda norma y/o procedimiento que regule esta política debe de estar alineada con lo establecido por el INEI en su Resolución Jefatural N° 0340-95-INEI sobre "Recomendaciones Técnicas para el Almacenamiento y Respaldo de la Información que se Procesan en las Entidades del Estado"

### Responsabilidad

Es responsabilidad de la Oficina de Informática el administrar las copias de respaldo, buscando minimizar los riesgos ante la presencia de una contingencia para lo cual debe elaborar normas y/o procedimientos que regulen esta política y establecer controles con las herramientas necesarias que le permitan verificar el cumplimiento de esta política y sus normas y/o procedimientos.

Es responsabilidad de todo usuario el velar por el cumplimiento de esta política y de las normas y/o procedimientos que la regulen. Asimismo está obligado a comunicar a la Oficina de Informática cualquier información sensible que se encuentre en las computadoras, a fin de establecer alguna forma de salvaguardar dicha información y evitar pérdidas de información en la organización ante alguna contingencia.

## **F. ADMINISTRACIÓN DE RECUPERACIÓN ANTE CONTINGENCIAS**

### Objetivo

El objetivo de esta política es establecer medidas necesarias que permitan responder eficazmente ante cualquier interrupción de los servicios informáticos. Estas medidas deben responder a un análisis de los posibles riesgos a los cuales pueden estar expuestos los recursos informáticos y comunicaciones de la institución.



### Alcance

Comprende a todos los componentes que conforman la plataforma informática de la organización, inclusive a equipos de respaldo al servicio informático. En cuanto al recurso humano involucra, dependiendo de la contingencia a todo el personal de la institución.

### Política

La Oficina de Informática es el ente encargado de elaborar y mantener actualizado el Plan de Contingencia que responde eficazmente a las necesidades de continuidad de los servicios informáticos. Este plan debe considerar: Plan de Emergencia que tiene como objetivo el contener el daño causado por un desastre, Plan de Respaldo que tiene el objetivo de mantener los servicios críticos de la operación y el Plan de Recuperación tiene el objetivo de restaurar temporal o permanente la capacidad de los servicios informáticos. Estos planes para garantizar su efectividad deben ser probados.

### Responsabilidad

Es responsabilidad de la Oficina de Informática, en conjunto con la Jefatura usuaria, la administración de recuperación ante la presencia de una contingencia, para lo cual debe elaborar los planes debidos, así como normas y procedimientos que regulen esta política y establecer controles con las herramientas necesarias que le permitan verificar el cumplimiento de esta política y sus normas y/o procedimientos.

## **G. ADMINISTRACIÓN DE DESARROLLO DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES.**

### Objetivo

El objetivo de esta política es registrar y controlar los desarrollos de proyectos de Tecnologías de Información y Comunicaciones, con la finalidad de reducir el riesgo por eventos imprevistos, de tal forma que el proyecto cumpla con las exigencias con que fue concebido.

### Alcance

Comprende todo desarrollo de proyectos de Tecnologías de Información y Comunicaciones realizados por el INEN y a todo desarrollo realizado por terceros que brindan el servicio a la institución.



### Política

La Oficina de Informática es el ente encargado de Administrar todos los desarrollos de Tecnologías de Información y Comunicaciones de la organización, por lo cual debe registrar desde el requerimiento inicial del usuario hasta el descarte o conclusión de los proyectos.

La Oficina de Informática es la encargada de supervisar y aprobar todo trabajo realizado por terceros, que esté relacionado en forma directa o indirecta con los recursos informáticos y comunicaciones, y aplicativos de la institución.

La Oficina de Informática debe contar con herramientas necesarias para el control de los proyectos y con una metodología para sus propios proyectos y que sirva de base para el desarrollo por servicio de terceros o proveedores que dan servicio a la institución.

### Responsabilidad

Es responsabilidad de la Oficina de Informática el velar por el cumplimiento de esta política, dar las normas y/o procedimientos que la regulen y de establecer controles.

## H. ADMINISTRACIÓN DE MANTENIMIENTO DE APLICACIONES

### Objetivo

El objetivo de esta política es registrar y controlar los mantenimientos de las aplicaciones, con la finalidad de reducir el riesgo por eventos imprevistos, de tal forma que el mantenimiento cumpla con las necesidades de los usuarios.

### Alcance

Comprende todo mantenimiento a las aplicaciones informáticas que se realizan para el INEN, inclusive aquellos mantenimientos realizados por terceros para el INEN.

### Política

La Oficina de Informática es el ente encargado de administrar todos los mantenimientos a las aplicaciones solicitadas por los usuarios, debiendo empezar desde el requerimiento inicial del usuario hasta el descarte o conclusión del mantenimiento.



La Oficina de Informática debe contar con herramientas necesarias para el control de los mantenimientos de aplicaciones.

### Responsabilidad

Es responsabilidad de la Oficina de Informática el velar por el cumplimiento de esta política, dar las normas y/o procedimientos que la regulen y de establecer controles que le permitan verificar el cumplimiento de esta política.



## GLOSARIO

### **Delito Informático**

Es toda aquella conducta ilícita, que hace uso de cualquier medio informático, susceptible de ser sancionada por el derecho penal.

Comportamiento ilegal o contrario a la ética o no autorizado, que concierne a un tratamiento automático de datos y/o transmisión de datos.

(Colección Seguridad de la Información, Delitos Informáticos - INEI)

### **Información Electrónica**

Toda información que para su transmisión hace uso de recursos o medios informáticos, y por lo general son producto de información procesada a través de sistemas de información.

### **Recursos Informáticos y Comunicaciones**

Dispositivos tecnológicos de hardware, software y comunicaciones destinados a soportar los procesos de los sistemas de información de una organización.

### **Contingencia**

Suceso o evento que puede suceder o no, y que significa un riesgo

### **Usuario**

Cualquier persona que utiliza una computadora. Por lo general se refiere a las personas que no pertenecen al personal técnico y que proporcionan entradas y reciben salidas de las computadoras.

