2013

POLÍTICA DE SEGURIDAD DE INFORMACIÓN EN EL IIAP

(Aprobada en sesión Ordinaria de Directorio N° 584 del 26 de Noviembre del 2013)

Iquitos, Noviembre 2013

Fecha	Autor	Versión	Notas
19 de julio de 2013	E. Maraza	0.1	Creado
18 de noviembre del 2013	A. Sanchez	0.2	Incorporando mejoras propuestas por el GTS

Instituto de Investigaciones de la Amazonía Peruana

Av. José A. Quiñones km 2.5

Apartado postal 784 – Iquitos, Perú

Teléfono: +51 (0)65 265515 / 265516

Fax: +51 (0)65 265527

Correo electrónico: sistemas@iiap.org.pe

www.iiap.org.pe

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN EL IIAP

1. FINALIDAD

   Implementar políticas de seguridad de la información para reducir el riesgo de que los activos de información estén expuestos a modificación, destrucción o divulgación de forma inadecuada en el Instituto de Investigaciones de la Amazonia Peruana.

2. OBJETIVO

   Establecer normas y procedimientos internos para implementar y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI) en el Instituto de Investigaciones de la Amazonia Peruana que permita garantizar la confidencialidad, integridad y disponibilidad de la información en los principales procesos de gestión del IIAP.

3. ALCANCE

   El presente manual de normas y procedimientos se aplica para todo el personal del Instituto de Investigaciones de la Amazonia Peruana (funcionarios, personal nombrado, servicios personales, CAS, etc.) y demás personas naturales o jurídicas que brindan bienes y/o servicios a la organización (empresas, consultores, etc.), alcanzando a los ciudadanos y empresas que hacen uso de los productos y/o servicios que brinda la institución.

4. BASE LEGAL

   4.1. Resolución Ministerial Nº 129-2012-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática.

   4.2. Resolución Ministerial Nº 246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información.

5. POLITICAS

   La Política de Seguridad de la Información del Instituto de Investigaciones de la Amazonia Peruana, expresada en el presente documento, establece las pautas que deben ser cumplidas por todo el personal de la institución y demás personas, con el fin de asegurar el adecuado nivel de confidencialidad, integridad y disponibilidad en su información.

   5.1. Seguridad Organizacional

      5.1.1. Grupo Técnico de Seguridad de Información

El Instituto de Investigaciones de la Amazonia Peruana constituirá un Grupo Técnico de Seguridad de Información para atender las temáticas relacionadas a la Seguridad de la Información, ante el cual se propondrán los planes, se informará de las acciones llevadas a cabo y se evaluaran los avances de dichos planes; estará conformado por; el Director del programa de BIOINFO: Coordinador del Grupo Técnico, un representante de cada uno de los 6 programas de investigación, un representante de las oficinas de gestión del Instituto. Teniendo entre sus principales funciones:

a) Revisar los resultados de los "análisis de riesgos" y aprobar los "controles de tratamiento de riesgo" que sean necesarios.
b) Verificar la efectividad en la implementación de las políticas de seguridad de información.
c) Evaluar y recomendar las sanciones en caso de "incidentes de seguridad", de conformidad con las normas vigentes.

5.1.2. Oficial de Seguridad de Información

El Instituto de Investigaciones de la Amazonia Peruana, deberá contar con un Oficial de Seguridad de Información cuya función principal será la implementación y mantenimiento de un Sistema de Gestión de la Seguridad de la Información en la Organización.(Ejecución, revisión, autorización y seguimiento).
Esta función estará a cargo del Jefe del Área de Informática y Redes del Programa BIOINFO, quien convocará y/o participará en grupos de trabajo de acuerdo a las necesidades y temáticas de seguridad de la información del IIAP.

5.1.3. Responsable de la información

El usuario interno que trabaja directamente con la información y su jefe inmediato serán considerados como responsable y titular de la información, respectivamente.

El área de Informática y Redes del Programa BIOINFO será responsable de mantener las condiciones de seguridad: confidencialidad, integridad y disponibilidad de la información en el IIAP.

5.2. Inventario de activos de información

5.2.1. Inventario de activos de información

El Instituto de Investigaciones de la Amazonia Peruana mantendrá actualizada la relación de activos de información (usuarios, formularios, documentación, sistemas, equipos, etc.) asociados a los principales procesos del mismo.

Se debe llevar un registro y control de todo el hardware, software, equipamiento de informática y comunicaciones u otros componentes

necesarios para el funcionamiento de los sistemas que sean adquiridos o arrendados, garantizando sus ubicaciones y protección adecuada, hasta su baja o retiro. Todo cambio o modificación en la relación de activos de información deberán de comunicarse al Área de Informática y Redes del Programa BIOINFO.

5.2.2. Clasificación de activos

Para cada proceso crítico de la organización se deberá efectuar una identificación y clasificación de los activos, relacionándolas con los usuarios titulares o con los responsables de la información, y con las dependencias internas o externas que intervienen.

5.2.3. Evaluación de riesgos de los activos

Los activos deberán ser evaluados a efectos de identificar las vulnerabilidades, amenazas y cuantificar el nivel de riesgo con el propósito de establecer los controles basados en el Código de Buenas Prácticas que establece la NTP ISO/IEC 17799:2007 EDI.

5.3. Seguridad del recurso humano

Todo personal nuevo del Instituto de Investigaciones de la Amazonia Peruana (funcionarios, servidores, CAS), que haya aprobado los procesos de selección de personal recibirá una capacitación sobre la seguridad de la información a fin de conocer, entender y asumir sus responsabilidades con respecto a la seguridad de la información, de conformidad con lo establecido en el presente documento. De igual manera se aplica a todo el personal vinculado a la entidad con anterioridad a la elaboración del presente documento. El incumplimiento de esta política de Seguridad de la Información implicara un proceso disciplinario y/o las acciones legales correspondientes, de acuerdo al marco legal vigente.

El término de contrato de trabajo con el Instituto de Investigaciones de la Amazonia Peruana implica el cumplimiento de los procesos de entrega de activos de información y remoción de privilegios sobre la plataforma tecnológica de la entidad.

5.4. Seguridad física y ambiental

5.4.1. Controles de acceso perimetral

Todo el personal del Instituto de Investigaciones de la Amazonia Peruana deberá portar constantemente y en un lado visible su fotocheck que lo acredita como personal de la entidad.

Todas las demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) que hagan su ingreso a las instalaciones de la entidad deberán estar adecuadamente identificadas y

deberán anunciar su llegada a través del personal de vigilancia a la institución.

Cualquier elemento u objeto (hardware o software) que entre o salga las diferentes instalaciones Instituto de Investigaciones de la Amazonia Peruana deberá ser anunciado al personal de vigilancia para que este proceda a hacer el registro correspondiente utilizando los formatos y procedimientos establecidos por el área de seguridad.

Las puertas de acceso al Datacenter, deberán permanecer cerradas en todo momento.

Todas las personas que ingresen a las áreas restringidas en la entidad, deberán cumplir los controles establecidos para el acceso específico a dichas áreas.

5.4.2. Controles ambientales

El Instituto de Investigaciones de la Amazonia Peruana proporcionara el ambiente adecuado para la conservación del respaldo de la información en medios magnéticos y equipos.

La Unidad de Logística de la Oficina General de Administración dispondrá de un sistema de video vigilancia para grabar en video las actividades en áreas de acceso público dentro o fuera de sus instalaciones, en áreas de acceso restringido y áreas donde se opera información confidencial o privada.

Todo el personal del Instituto de Investigaciones de la Amazonia Peruana que utilice estaciones de trabajo para la realización de su labor, deberá acoger como practica permanente el bloqueo de la pantalla al ausentarse de su puesto de trabajo, cuidando la confidencialidad de la información.

Las estaciones de trabajo de los usuarios finales serán programadas para ser desactivadas automáticamente, en caso superen un tiempo de inactividad determinada, y requerir de nuevo el ingreso de la clave de acceso.

5.4.3. Soporte y/o Mantenimiento

El Instituto de Investigaciones de la Amazonia Peruana identificará y establecerá esquemas de soporte y/o mantenimiento para cada uno de los componentes de su plataforma tecnológica, asimismo la periodicidad de acuerdo a sus características técnicas.

5.4.4. Bóveda de Seguridad

La entidad deberá contar con un ambiente asignado, de acuerdo a estándares, para la custodia de activos de información como licencias de software, cintas u otros medios de información critica.

5.5. Administración de comunicaciones y operaciones

5.5.1. Documentación operativa

Todos los procedimientos operativos del Instituto de Investigaciones de la Amazonia Peruana, estarán adecuadamente documentados, actualizados y a disposición de los usuarios competentes.

5.5.2. Control de cambios

Cualquier cambio a la plataforma tecnológica del Instituto de Investigaciones de la Amazonia Peruana deberá ser completamente documentado y controlado por el Área de Informática y Redes del Programa BIOINFO, los cambios en la plataforma de las estaciones de trabajo deberán ser autorizados por la misma área.

Cualquier cambio a ser realizado en las aplicaciones o sistemas informáticos existentes, desarrollados para la operación normal del Instituto de Investigaciones de la Amazonia Peruana, deberá ser requerido por el área usuaria competente, correspondiendo al Área de Informática y Redes del Programa BIOINFO mantener su documentación y sus versiones controladas.

5.5.3. Uso de la Tecnología

El Área de Informática y Redes del Programa BIOINFO identificará, evaluará y establecerá los criterios de utilización de los nuevos recursos tecnológicos y estándares adecuados para su óptima administración.

Los recursos informáticos del Instituto de Investigaciones de la Amazonia Peruana deberán ser utilizados únicamente para propósitos propios de la institución.

5.5.4. Servicios de red

El Instituto de Investigaciones de la Amazonia Peruana, a través del Área de Informática y Redes del Programa BIOINFO, mantendrá un monitoreo permanente sobre la red interna, implementando para ello las herramientas que permitan detectar, prevenir y recuperarse inmediatamente ante un ataque externo o falla.

La entidad mantendrá actualizada, con la debida aprobación del Área de Informática y Redes del Programa BIOINFO, una lista de usuarios según categorías de acceso para la navegación en la Intranet, Extranet e Internet.

5.5.5. Software

La institución a través del Área de Informática y Redes del Programa BIOINFO efectuara revisiones periódicas al cumplimiento de la normatividad existente en materia de propiedad intelectual.

Todo el personal del Instituto de Investigaciones de la Amazonia Peruana y demás personas (funcionarios, servidores, CAS) tienen PROHIBIDO instalar o utilizar software o productos sin licencias no autorizadas por la entidad. Se exceptúan de esta política los productos de software libre o que sean soportados con certificado de propiedad de licencia de terceros o que hayan sido resultado de desarrollo propio, en cuyo caso, cualquier instalación de software debe ser solicitada y obtenida de acuerdo a los procedimientos de adquisiciones existentes, a través del Área de Informática y Redes del Programa BIOINFO.

5.5.6. Computación Móvil

El uso de equipos portátiles asignados al personal autorizado del Instituto de Investigaciones de la Amazonia Peruana deberá cumplir con las recomendaciones de seguridad e instrucciones de uso, a ser emitidas por el Área de Informática y Redes del Programa BIOINFO.

Los equipos portátiles u otros dispositivos inteligentes que requieran conectarse a la red del Instituto de Investigaciones de la Amazonia Peruana, previamente deberán pasar por una verificación y autorización por parte del Área de Informática y Redes del Programa BIOINFO.

5.5.7. Backups o respaldos de información

Toda la información del Instituto de Investigaciones de la Amazonia Peruana debe ser respaldada por medio de copias de seguridad siguiendo el procedimiento adecuado.

El respaldo de la información de las estaciones de trabajo es responsabilidad de cada usuario, por lo tanto ningún trabajador podrá borrar información que pertenece a la institución de la computadora a su cargo. Para ello deberá mantener depurada la información de sus archivos públicos, como mejor practica para la optimización del uso de los recursos que entrega la entidad a su personal.

Es responsabilidad del Área de Informática y Redes del Programa BIOINFO, definir las políticas de respaldo que incluyen los periodos de retención, las frecuencias y demás, de los Backups que permitan la restauración de los datos y la consulta a información histórica.

5.5.8. Control de código malicioso

El Instituto de Investigaciones de la Amazonia Peruana contara permanentemente con un sistema efectivo de seguridad perimetral que

permitan prevenir, detectar y corregir intrusiones o intentos de ingreso no autorizado, el cual será administrado por el Área de Informática y Redes del Programa BIOINFO.

Es responsabilidad de todo el personal del Instituto de Investigaciones de la Amazonia Peruana y demás personas (funcionarios, servidores, CAS), revisar que todos los medios magnéticos extraíbles sean chequeados con un antivirus provisto por la entidad, antes de introducirlos en los computadores personales o equipos servidores de la entidad.

5.5.9. Responsabilidad operativa

El Área de Informática y Redes del Programa BIOINFO se responsabilizará de la continuidad de la operación de los equipos y sistemas de computo para lo cual adoptara las mejores prácticas.

5.6. Controles de acceso

5.6.1. Administración de usuarios

El Área de Informática y Redes del Programa BIOINFO del IIAP establecerá los roles y privilegios para la administración y uso de cada componente de la plataforma tecnológica o para el acceso dentro de cada una de las aplicaciones.

El personal del Instituto de Investigaciones de la Amazonia Peruana tendrá un usuario y contraseña única de identificación ante el sistema y será responsable de todo registro a su nombre.

Está prohibido intentar ingresar a los servicios de computo y comunicaciones utilizando el nombre de usuario y clave de otro personal de la institución o de otras personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros). Las cuentas que no hayan sido utilizadas en los últimos noventa (90) días serán inhabilitadas o eliminadas, dependiendo del caso.

La creación, eliminación y revisión de privilegios de los usuarios de la red y las aplicaciones del Instituto de Investigaciones de la Amazonia Peruana deberán ser revisadas regularmente por el Área de Informática y Redes del Programa BIOINFO.

La Unidad de Personal de la Oficina General de Administración y/o áreas correspondientes deberán enviar oportunamente al Área de Informática y Redes del Programa BIOINFO, la lista actualizada de altas, bajas, vacaciones, licencias, inhabilitaciones, etc., de todo el personal y demás personas (funcionarios, servidores, CAS) autorizadas, a fin de llevar un control y mantenimiento de las cuentas de usuario.

5.6.2. Contraseñas

El personal del Instituto de Investigaciones de la Amazonia Peruana deberá crear una contraseña que cumpla con las características de seguridad (Incluir letras, números, mayúsculas y minúsculas); cuyos esquemas y periodicidad de cambio serán definidos por el Área de Informática y Redes del Programa BIOINFO.

Es responsabilidad directa del personal del Instituto de Investigaciones de la Amazonia Peruana y demás personas (funcionarios, servidores, CAS) el velar por la confidencialidad y buen uso de su contraseña.

5.6.3. Controles de acceso de red

El Área de Informática y Redes del Programa BIOINFO del IIAP garantizará a la entidad que el personal del IIAP y demás personas autorizadas (funcionarios, servidores, CAS) reportadas por la Unidad de Personal de la Oficina General de Administración y/o áreas correspondientes como ausentes por motivo de viaje, vacaciones, licencias, etc., puedan acceder a la red interna de la institución para desarrollar actividades laborales o mantener comunicación con la entidad.

Ningún miembro del personal de informática tendrá acceso a los datos de los sistemas en producción, en modalidad diferente a la de consulta, a excepción del Administrador de la Base de Datos. Excepto, cuando se realice por expresa autorización del Área de Informática y Redes del Programa BIOINFO del IIAP.

El personal del Instituto de Investigaciones de la Amazonia Peruana y demás personas (funcionarios, servidores, CAS) autorizadas en ningún caso tendrán acceso de escritura a los datos de los sistemas en producción por fuera de las interfaces de usuarios

Para cubrir eventualidades sobre el acceso a la red causadas por ausencia imprevista, por razones de caso fortuito o fuerza mayor del personal, se recurrirá al uso de perfiles de acceso a los servicios y datos que permitan la continuidad del desarrollo de las labores del personal, para lo cual deberán ser reportados al jefe inmediato y al Responsable de Seguridad o quien haga sus veces.

5.6.4. Controles de acceso a aplicaciones

Las aplicaciones incluirán un adecuado control de acceso basado en el análisis de las funciones que la aplicación tiene desarrollada y las autorizaciones por grupos de usuarios, roles y perfiles.

5.7. Sistemas de información

5.7.1. Requerimientos de seguridad

Las nuevas aplicaciones que se pondrán en operación en la entidad deben cumplir los requerimientos de seguridad mínimo establecidos para asegurar confidencialidad, integridad y disponibilidad en la información que manejan. Para ello, el Área de Informática y Redes del Programa BIOINFO es responsable de poner y mantener a disposición de la entidad la infraestructura tecnológica más conveniente de acuerdo a sus requerimientos y lo que ofrece el mercado.

5.7.2. Datos para pruebas

El Instituto de Investigaciones de la Amazonia Peruana mantendrá por separado sus sistemas en producción, desarrollo y calidad, y en cada uno de ellos mantendrá únicamente los elementos que se consideren adecuados con el fin de mitigar los riesgos. Es responsabilidad del Área de Informática y Redes del Programa BIOINFO asegurar que los datos dispuestos para la realización de los procesos de calidad y desarrollo cuenten con la debida protección para minimizar los riesgos con respecto a la confidencialidad

5.7.3. Análisis de Vulnerabilidades

Es responsabilidad del Área de Informática y Redes del Programa BIOINFO en efectuar pruebas de vulnerabilidades a los componentes de la plataforma tecnológica para determinar el nivel de riesgos existentes y adoptar las medidas de seguridad.

5.7.4. Administración de sistemas de información

El Instituto de Investigaciones de la Amazonia Peruana deberá cumplir el esquema general de ciclo de vida de los proyectos, de acuerdo a la metodología basada en la "Norma Técnica peruana NTP ISO/IEC 12207:2006 Tecnología de la Información. Procesos del ciclo de vida del software. 2º Edición", sobre el Ciclo de Desarrollo del Software, esto es tanto para el mantenimiento de aplicaciones en producción, calidad o desarrollos nuevos.

5.7.5. Cifrado

En los medios y transmisiones electrónicas que el Instituto de Investigaciones de la Amazonia Peruana determine, se deberán establecer políticas y esquemas de cifrado o encriptación que cumplan los requerimientos específicos para tal fin.

5.8. Incidentes de seguridad

5.8.1. Reporte de incidentes y eventos de seguridad

Todo el personal del Instituto de Investigaciones de la Amazonia Peruana debe reportar cualquier incidente de seguridad que detecte al oficial de Seguridad de la información de forma Oportuna.

5.8.2. Administración de incidentes de seguridad

El Oficial de Seguridad de Información o quien haga sus veces debe realizar el debido estudio y seguimiento de todos los incidentes de seguridad, valiéndose de la asistencia de todos los usuarios involucrados cuando este lo requiera, para lo cual debe mantener actualizadas las estadísticas de mantenimiento de emergencia, clasificadas en técnicas y de usuario, siendo estas reportadas a la Gerencia Estratégica.

5.9. Continuidad de operaciones

5.9.1. Planeación del plan de continuidad de operaciones

El Instituto de Investigaciones de la Amazonia Peruana diseñará y mantendrá vigente un Plan de Continuidad de Operaciones que atienda los requerimientos de Seguridad de la información en la entidad según el análisis de riesgos determinado para tal fin.

5.9.2. Mantenimiento del Plan de Continuidad de Operaciones

La entidad realizara pruebas periódicas y mantenimiento al Plan de Continuidad de Operaciones. La entidad podrá contar con un contrato de custodia externa de la información, como parte del plan de continuidad de operaciones.

5.10. Cumplimiento

5.10.1. Protección Legal

El Instituto de Investigaciones de la Amazonia peruana, en relación a la protección legal de los derechos de autor contempla las siguientes políticas:

a) Política de uso y derecho de autor de software

Administrar los activos de software para lograr el máximo beneficio para el Instituto de Investigaciones de la Amazonia Peruana con la finalidad de: adquirir, distribuir y usar software de acuerdo a lo establecido en el Decreto Supremo Nº 013-2003-PCM y las modificatorias posteriores.

b) Políticas y procedimiento de adquisición

La ejecución de un proceso formal de adquisición de software se deberá iniciar con el requerimiento del área usuaria con la asistencia técnica del Área de Informática y Redes del Programa BIOINFO, siguiendo las políticas, normas y procedimientos internos establecidos para las compras de bienes y/o servicios.

c) Políticas y procedimientos para la capacitación

El área de Informática y Redes del Programa BIOINFO es la encargada de administrar el uso del software adquirido o desarrollado por el Instituto de Investigaciones de la Amazonia Peruana, en ese sentido está encargada de su instalación, actualización y/o remoción.

Políticas y procedimientos para la capacitación

El área de Informática y Redes del Programa BIOINFO en coordinación con la Unidad de Personal de la Oficina General de Administración , ofrecerá capacitación dirigida al personal del Instituto de Investigaciones de la Amazonia Peruana sobre el uso de software: Ofimática, Gestión Documentaria y uso de Aplicativos de importancia institucional.

d) Políticas de disposición del software

El área de Informática y Redes del Programa BIOINFO es la encargada de detectar y eliminar el software obsoleto o que no cuente con licencia de uso.

5.10.2. Normatividad

La presente política de seguridad de la información del Instituto de Investigaciones de la Amazonia Peruana fue diseñada para ajustarse o exceder, sin contravenir, las medidas de protección establecidas en las leyes y regulaciones vigentes.

Si el personal del Instituto de Investigaciones de la Amazonia Peruana u otra persona autorizada (funcionarios, servidores, CAS) consideran que alguna política de seguridad de información está en conflicto, por defecto o exceso, con las leyes y regulaciones existentes, lo debe reportar en forma inmediata al Oficial de Seguridad de Información.

5.10.3. Auditoria en seguridad informática

El área de Informática y Redes del Programa BIOINFO deberá establecer controles de seguridad al momento de la implantación de las normas y sistemas de gestión de la seguridad de la información, las cuales servirán para las auditorias que correspondan.

Instituto de Investigaciones
de la Amazonía Peruana

Instituto de Investigación de la Amazonia Peruana - IIAP
Programa de Investigación en Información de la Biodiversidad Amazónica
BIOINFO
05 DIC 2013
Hora: 9:30 a
Expediente: 9

MEMORANDUM Nº 827-2013-IIAP-GE

A	:	**LUIS EXEQUIEL CAMPOS BACA** Director de BIOINFO
ASUNTO	:	Aprueban Política de Seguridad de la información en el IIAP.
REF.	:	Memorando N° 45-2013-IIAP-BIOINFO/AJASC
FECHA	:	Iquitos, 03 de diciembre de 2013

Por el presente comunico a usted que el Directorio del IIAP, en su Sesión Ordinaria Nº 584 de fecha 26 de noviembre de 2013, llevada a cabo en la ciudad de Tarapoto, luego de analizar los documentos de la referencia, acordó: aprobar la Política de Seguridad de la Información en el instituto de Investigaciones de la Amazonía Peruana, propuesta por el Programa de BIOINFO mediante memorando N° 45-2013-IIAP-/AJAS.

Encargar a la Dirección de BIOINFO la implementación y difusión de la presente política, a través del intranet y de la página web institucional.

Atentamente,

Instituto de Investigaciones de la Amazonía Peruana
Gerencia Estratégica

ROGER W. BEUZEVILLE ZUMAETA
Gerente General

Cc. P,
Archivo

Instituto de Investigaciones de la Amazonia Peruana
BIOINFO

Iquitos,
Pase: Américo,
Para: Implementar y difundir lo presente política

Dr. Luis Exequiel Campos Baca
Director BIO

Instituto de Investigaciones de la Amazonía Peruana
GERENCIA GENERAL
RECIBIDO
18 NOV. 2013
Nº Exp. 2269 Hora: 8:00
Firma:

910.
Hora: 12:30
Expediente:

MEMORANDO Nº 45-2013-IIAP-BIOINFO/AJASC

A : Dr. Luis Campos Baca

Director de Bioinfo

ASUNTO : Remite política de seguridad de la información en el IIAP

FECHA : Iquitos, 18 de noviembre del 2013

Por la presente le remito la Política de seguridad de la información en el IIAP elaborada y mejorada al interior del Grupo Técnico de Seguridad de la Información.

En cumplimiento de la Resolución Ministerial N° 129-2012-PCM, que orienta al interior del Sector público, la implementación del Sistema de Gestión de la Seguridad de la información, el Programa BIOINFO ha liderado la elaboración de la Política de seguridad de la información en el IIAP la misma que se basa en el Norma Técnica Peruana ISO/IEC 27001:2008, norma de obligatorio cumplimiento al interior del Sistema Nacional de Informática.

Finalmente el suscrito sugiere se remita la presente Política de Seguridad de la Información en el IIAP a la Alta Dirección del Instituto a efectos de su revisión y aprobación como Política Institucional Oficial.

Agradeciendo la atención a la presente, le saluda.

Cordialmente,

Ing Américo Sánchez Cosavalente
Investigador de Bioinfo

INSTITUTO DE INVESTIGACIONES DE LA AMAZONIA PERUANA
Gerencia Estratégica
19.11.2013
Sra. Lalvi

c.c: Archivo

DIRECTORIO

Roger Rengifo
El Director