REPÚBLICA DEL PERÚ

RESOLUCIÓN DE PRESIDENCIA Nº 114 -2017-CONCYTEC-P

Lima, 20 SET. 2017

VISTOS: El Acta Nº 01-2017-SGSI del Comité de Gestión de Seguridad de la Información, el Informe Nº 002-2017-CONCYTEC-CSGSI de la Oficial de Seguridad de la Información, el Informe Nº 052-2017-CONCYTEC-OGA-OTI-MAS de la Oficina de Tecnologías de Información, el Memorando Nº 436-2017-CONCYTEC-OGA de la Oficina General de Administración, el Informe Nº 052-2017-CONCYTEC-OGPP-OMGC de la Oficina de Modernización y Gestión de la Calidad y el Informe Nº 187-2017-CONCYTEC-OGPP de la Oficina General de Presupuesto, y;

CONSIDERANDO:

Que, el Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica – CONCYTEC, es un organismo público técnico especializado adscrito a la Presidencia de Consejo de Ministros, con personería jurídica de derecho público interno y autonomía científica, administrativa, económica y financiera, conforme a lo establecido en la Ley Nº 28613 y los Decretos Supremos Nº 058-2011-PCM y Nº 067-2012-PCM;

Que, la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición" (en adelante la Norma Técnica) fue aprobada por Resolución Nº 129-2014-DNB-INDECOPI;

Que, mediante Resolución Ministerial Nº 004-2016-PCM se aprueba el uso obligatorio de la Norma Técnica, en todas las entidades integrantes del Sistema Nacional de Informática;

Que, conforme a Resolución de Presidencia Nº 079-2016-CONCYTEC-P, de fecha 20 de mayo de 2016, se constituyó el Comité de Gestión de Seguridad de la Información del Pliego CONCYTEC (en adelante, el Comité), estableciéndose entre sus funciones, revisar la propuesta de Política de Seguridad de la Información del Pliego CONCYTEC elaborada por la Oficina de Tecnologías de Información y proponerla a la Alta Dirección para su aprobación;

Que, el Literal a) del Artículo 5-A de la Resolución Ministerial Nº 004-2016-PCM, articulo que fue incorporado por el Articulo 2 de la Resolución Ministerial Nº 166-2017-PCM, señala que corresponde al Comité de Gestión de Seguridad de la Información el proponer la política y objetivos de seguridad de la información alineados con el Plan Estratégico Institucional, con la Política Nacional de Gobierno Electrónico y regulación en el ámbito de seguridad de la información;

Que, conforme consta en el Acta Nº 01-2017-SGSI de fecha 6 de julio de 2017, el Comité acordó que una vez revisado se gestionará la aprobación de la Política de Seguridad de la Información del Pliego CONCYTEC;

Que, mediante Informe Nº 002-2017-CONCYTEC-CSGSI, la Oficial de Seguridad de la Información remite la Política de Seguridad de la Información para el Pliego CONCYTEC, debidamente visada por los miembros del Comité, solicitando se realice las acciones correspondientes para la aprobación de la misma;

Que, a través del Memorando Nº 436-2017-CONCYTEC-OGA, la Oficina General de Administración y Finanzas remite el Informe Nº 052-2017-CONCYTEC-OGA-OTI-MAS, que cuenta con la conformidad del Jefe (e) de la Oficina de Tecnologías de Información otorgada mediante Proveído Nº 122-2017-OTI, con la cual se remite la propuesta de Política de Seguridad de la Información para el Pliego CONCYTEC, solicitando se tramite su aprobación;

Que, mediante Informe Nº 052-2017-CONCYTEC-OGPP-OMGC, la Oficina General de Modernización y Gestión de la Calidad, otorga su conformidad a la aprobación de la Política de Seguridad de la Información; la misma que cuenta con la conformidad de la Oficina General de Planeamiento y Presupuesto, otorgada a traves del Informe Nº 187-2017-CONCYTEC-OGPP;

Que, en consecuencia, considerando lo informado por los órganos técnicos competentes, corresponde emitir el respectivo acto de administración con el cual se apruebe la Política de Seguridad de la Información del Pliego CONCYTEC;

Con la visación de la Jefa de la Oficina General de Administración, del Jefe (e) de la Oficina General de Planeamiento y Presupuesto, de la Jefa (e) de la Oficina de General de Asesoría Jurídica y del Encargado de las funciones de la Oficina de Tecnologías de Información;

De conformidad con lo dispuesto en la Resolución Ministerial Nº 004-2016-PCM modificada por la Resolución Ministerial Nº 166-2017-PCM; la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", aprobada por Resolución Nº 129-2014-DNB-INDECOPI; la Ley N° 28613, Ley del Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica - CONCYTEC, y su Reglamento de Organizaciones y Funciones aprobado por Decreto Supremo N° 026-2014-PCM;

SE RESUELVE:

Artículo 1.- Aprobar la Política de Seguridad de la Información del Pliego Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica - CONCYTEC, que en Anexo forma parte integrante de la presente Resolución.

Artículo 2.- Encargar al Responsable del Portal de Transparencia la publicación de la presente Resolución y su Anexo en el Portal Institucional del CONCYTEC.

Regístrese y comuníquese.

Dra. Fabiola León-Velarde Servetto
Presidenta
Consejo Nacional de Ciencia, Tecnología
e Innovación Tecnológica
CONCYTEC

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL PLIEGO CONCYTEC

P0.01

CONCYTEC - A. LA ROSA SÁNCHEZ - OFICINA GENERAL DE ADMINISTRACIÓN

CIENCIACTIVA - FONDO NACIONAL DE DESARROLLO CIENTÍFICO, TECNOLÓGICO Y DE INNOVACIÓN TECNOLÓGICA - Carlos Chois Pimentel - Unidad de Tecnologías de la Información

CONCYTEC - P. VÁSQUEZ - OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

CONCYTEC - M. ACUÑA - OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

CONCYTEC - J. FERNÁNDEZ

CONCYTEC - A. NARCISO - OFICINA GENERAL DE ASESORÍA JURÍDICA

ELABORADO POR:	FECHA	FIRMA
Marisol Acuña Santivañez Oficial de Seguridad de la Información	19.07.17	
REVISADO POR:		
Aida La Rosa Sánchez Bayes de Lopez Jefe de la Oficina General de Administración	19. 7.17	
Johan Fernández Jibaja Jefe (e) de la Oficina General de Planeamiento y Presupuesto	19/7/2017	
Anmary Narciso Salazar Jefe (e) de la Oficina General de Asesoría Jurídica	19/7/2017	
Percy Vasquez Machicao Jefe (e) de la Oficina de Tecnologías de Información	19/07/17	
Carlos Chois Pimentel Responsable (e) de la Unidad de Tecnología de Información - FONDECYT	19/07/17	
APROBADO POR:		
Fabiola María León-Velarde Servetto Presidenta del CONCYTEC		

Registro de Modificaciones			
Revisión	Fecha	Descripción de la modificación	Autor de la modificación
01		Primer Documento	No procede
02			
03			
04			

ÍNDICE

CONCYTEC - A. LA ROSA SÁNCHEZ - OFICINA GENERAL DE ADMINISTRACIÓN

CONCYTEC - P. VÁSQUEZ - OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

CIENCIACTIVA - FONDO NACIONAL DE DESARROLLO CIENTÍFICO, TECNOLÓGICO Y DE INNOVACIÓN TECNOLÓGICA - Carlos Chois Pimentel - Unidad de Tecnologías de la Información

CONCYTEC - M. ACUÑA - OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

CONCYTEC - J. FERNANDEZ - OFICINA GENERAL DE PLANEAMIENTO Y PRESUPUESTO

CONCYTEC - NARCISO - OFICINA GENERAL DE ASESORÍA JURÍDICA

POLITICA DE SEGURIDAD DE LA INFORMACIÓN DEL PLIEGO CONCYTEC

1. DECLARACIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

El pliego Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica, en adelante CONCYTEC, tiene como activo principal la información y los activos de tratamiento de la información tales como, documentos, licencias, aplicativos informáticos, equipos de procesamiento, almacenamiento, telecomunicaciones, y la seguridad de la información son de vital importancia para el desarrollo de su gestión y cumplimiento de su misión, visión, procesos, funciones, planes y objetivos estratégicos y funcionales, por lo tanto, se compromete a implantar una cultura en seguridad de la información e implementar controles, procedimientos, metodologías, buenas prácticas y tecnología adecuada que prevenga la ocurrencia de incidencias que atenten contra la confidencialidad, integridad y disponibilidad de la información.

2. INTRODUCCIÓN:

La Política de Seguridad de la Información ha sido elaborada tomado como marco de referencia la NTP–ISO/IEC 27001:2014, aprobada con Resolución Ministerial N° 004-2016-PCM, cuya finalidad principal es asegurar la confidencialidad, integridad y disponibilidad de la información gestionada en la entidad.

Así también se establecen las directrices que atenúan los riesgos de seguridad de la información y permiten proteger este recurso de las diversas amenazas que impiden garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos institucionales.

La seguridad de la información se logra implementando un conjunto adecuado de controles, que abarcan normativas, políticas, prácticas, procedimientos, estructuras organizacionales y tecnologías.

En el Anexo A – Glosario de Definiciones, se presentan las definiciones de los términos utilizados en este documento, con el objeto de poder unificar el entendimiento de los mismos.

3. OBJETIVO:

Establecer el marco general de la seguridad de la información que permita fortalecer los niveles de seguridad de los recursos de información del CONCYTEC y la tecnología utilizada para su procesamiento, frente a todo tipo de amenazas deliberadas o accidentales.

4. BASE LEGAL:

4.1 Ley Nº 27269 –Ley de Firmas y Certificados Digitales y su reglamento.
4.2 Texto Único Ordenado de la Ley N° 28303, Ley Marco de Ciencia, Tecnología e Innovación Tecnológica, aprobado por el Decreto Supremo N° 032-2007-ED.
4.3 Ley N° 27309, Ley que incorpora los delitos informáticos al Código Penal.
4.4 Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, aprobado mediante Decreto Supremo Nº 072-2003-PCM y sus modificatorias.
4.5 Ley Nº 27815, Ley del Código de Ética de la Función Pública aprobado mediante Decreto Supremo N° 033-2005-PCM.

CONCYTEC - A. LA ROSA SANCHEZ - OFICINA GENERAL DE ADMINISTRACIÓN
CONCYTEC - P. VÁSQUEZ - OFICINA DE TECNOLOGÍAS DE INFORMACIÓN
CONCYTEC - M. ACUÑA - OFICINA DE TECNOLOGÍAS DE INFORMACIÓN
CONCYTEC - J. FERNANDEZ - OFICINA GENERAL DE ASESORÍA JURÍDICA
CONCYTEC - M. NARCISO - OFICINA GENERAL DE ASESORÍA JURÍDICA
CIENCIACTIVA - FONDO NACIONAL DE DESARROLLO CIENTÍFICO, TECNOLÓGICO Y DE INNOVACIÓN TECNOLÓGICA - Carlos Chois Sarmentel - Unidad de Tecnologías de la Información

4.6 Ley Nº 28613, Ley del Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica.
4.7 Ley Nº 29733 – Ley de Protección de Datos Personales, y su reglamento.
4.8 Resolución Direccional Nº 001-2013-JUS/DGPDP que aprueba formularios para la inscripción de banco de datos personales de administración privada por persona natural, la administración privada por persona jurídica y de la administración publica
4.9 Resolución Ministerial N° 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 2ª. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
4.10 Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
4.11 Resolución Ministerial Nº166-2017-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001-2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática. Modificatoria del Articulo 5 de la Resolución Ministerial N° 004-2016-PCM
4.12 Resolución de Presidencia N° 079-2016-PCM que conforma el Comité de Gestión de Seguridad de la Información del Pliego CONCYTEC.

5. ALCANCE:

La Política de Seguridad de la Información es de aplicación y cumplimiento por el Pliego: CONCYTEC y las personas contratadas por estas bajo cualquier régimen contractual, que interactúan de manera habitual u ocasional, que accedan a información y/o a los recursos informáticos, en el desarrollo de sus actividades.

6. ROLES Y RESPONSABILIDADES

6.1 Presidencia del CONCYTEC

a. Aprobar la Política de Seguridad de la Información del Pliego CONCYTEC y sus futuras modificaciones, a propuesta del Comité de Gestión de Seguridad de la Información del Pliego CONCYTEC.

6.2 Comité de Gestión de Seguridad de la Información del pliego CONCYTEC

a. Proponer la política y objetivos de seguridad de la información alineados con el Plan Estratégico Institucional, con la Política Nacional de Gobierno Electrónico y regulación en el ámbito de seguridad de la información.

b. Promover y gestionar la implementación del Sistema de Gestión de Seguridad de la Información.

c. Promover la gestión de seguridad de la información en los procesos y cultura organizacional.

d. Gestionar la asignación del personal y recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información.

e. Difundir la importancia de una efectiva gestión de seguridad de la información a las partes interesadas, en conformidad con los requisitos del Sistema de Gestión de Seguridad de la Información.

f. Evaluar el desempeño del Sistema de Gestión de Seguridad de la Información.

g. Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.

6.3 Presidente del Comité de Gestión de Seguridad de la Información:

a. Dirigir las sesiones del Comité de Gestión de Seguridad de la Información.
b. Proponer estrategias y soluciones específicas de los controles necesarios para implementar las políticas de seguridad de la información establecidas y la debida solución de las situaciones de riesgo detectadas.

6.4 Oficial de Seguridad de la Información

a. Formular y proponer a los miembros del comité de seguridad de la información las políticas, objetivos, lineamientos, planes, roles y funciones necesarias para la gestión técnica y efectiva de la seguridad de la información
b. Coordinar la ejecución de iniciativas, proyectos y/o actividades especializadas en Seguridad de la información y de sus resultados
c. Mantener coordinación con todas las unidades orgánicas en temas relacionados con la seguridad de la información.
d. Coordinar con las unidades orgánicas la implementación de los controles de seguridad de la información para los procesos a su cargo
e. Identificar las necesidades de capacitación, difusión y sensibilización en seguridad de la información.
f. Promover la realización las auditorías especializadas relacionadas a la seguridad de la información.

6.5 Secretario Técnico del Comité de Gestión de Seguridad de la Información

a. Convocar, a solicitud del Presidente, a sesiones del Comité de Seguridad de la Información
b. Elaborar el Acta de Sesión y remitir para rubrica a los miembros el comité
c. Custodiar la Actas y la documentación de todas las actuaciones del comité.
d. Efectuar las acciones que correspondan para la implementación de los acuerdos adoptados por el comité.

6.6 Directores, Sub Directores y Jefes de Oficina

a. Aceptar por escrito la adhesión a la presente política y objetivos de la Seguridad de la Información.
b. Incentivar a todo el personal a su cargo, el cumplimiento permanente de la política de seguridad de la Información.
c. Informar al Oficial de Seguridad de la Información de situaciones que ameriten una investigación o revisión.
d. Autorizar al personal a su cargo, la asistencia a las capacitaciones sobre seguridad de la Información que se programen.
e. Asistir a las convocatorias de reuniones de trabajo o asignar a un responsable cuando se solicite.
f. Atender los requerimientos de información cuando el Oficial de Seguridad de la Información lo solicite.

6.7 Personal Interno y Externo (bajo toda modalidad de contratación)

a. Cumplir con lo estipulado en la presente política.
b. Firmar el Compromiso de Confidencialidad o no divulgación.
c. Reportar eventos, incidentes y debilidades de seguridad de la información de acuerdo a los procedimientos establecidos por la entidad.

7. DISPOSICIONES GENERALES:

7.1 El Pliego CONCYTEC garantizará la aplicación de las medidas de seguridad de la información que se establecen y optimizará su gestión mediante el Comité de Gestión de Seguridad de la Información, el Oficial de Seguridad de la Información, y los propietarios y custodios de la información.

7.2 La Unidad de Informática o quien haga sus veces en el FONDECYT, será considerada unidad de apoyo al Comité de Gestión de Seguridad de la Información del Pliego CONCYTEC.

7.3 La Alta Dirección reconoce como activos de información, a la información contenida en cualquier medio y sistemas que la soportan. Por tanto la Política de Seguridad de la Información es de aplicación obligatoria para todas las personas contratadas por el CONCYTEC bajo cualquier régimen contractual, que interactúan de manera habitual u ocasional, que accedan a información sensible y/o a los recursos informáticos, en el desarrollo de sus actividades.

7.4 Cuando exista la necesidad de otorgar algún acceso lógico y físico o conexión a la red interna a personas externas (locadores de servicio), deberá ser comunicada y autorizada de acuerdo a los procedimientos que se establezcan.

7.5 Todos los contratos con personas laborales o de servicios con personas (naturales o jurídicas) para la administración, desarrollo, mantenimiento o control de los sistemas de información, redes y/o ambientes de procesamiento de informacióndeberá incluir o una clausula o un Acuerdo de Confidencialidad según corresponda.

7.6 Los contratos para los cuales se transfiere la responsabilidad de la seguridad de la información a un tercero (u outsourcing), deberán dejar en forma explícita el compromiso por parte de este; así como la aplicación de los controles de seguridad necesarios en la medida en que el Pliego CONCYTEC le ha transferido dicha responsabilidad.

7.7 La presente política será revisada anualmente o cuando sea necesario según normativa por el Comité de Gestión de Seguridad de la Información, para establecer la necesidad de actualización.

7.8 El Oficial de Seguridad de la Información será la persona autorizada a responder las consultas respecto a temas asociados a la seguridad de la información, previa autorización del Comité de Gestión de Seguridad de la Información.

8. LINEAMIENTOS DE LA POLÍTICA:

8.1 Gestión de activos de información

Objetivo: Garantizar que los activos de información reciban un apropiado nivel de protección y uso, en función al grado de sensibilidad que presenten.

a. Todos los activos de información deberán ser identificados, clasificados, administrados e inventariados, de acuerdo a los niveles que se establezcan.
b. Toda adquisición de cualquier naturaleza que haga la entidad en materia de hardware, software, servicios en temas informáticos e información, debe tener un control de su ubicación, asignación, estado y aspectos técnicos, a través de la Unidad Informática o la dependencia competente.
c. La reasignación o baja de equipos informáticos que contengan dispositivos de almacenamiento de información del CONCYTEC, estará a cargo de su Unidad de Informática, y deberá comprobarse que dicha información haya sido sobrescrita o eliminada antes de su reasignación o baja.

8.2 Seguridad relacionada al personal:

Objetivo: Asegurar que el personal interno y externo, entienda sus responsabilidades y que estas sean adecuadas a los roles para los cuales han sido contratados, reduciendo el fraude, estafa o mal uso de la información y de las instalaciones.

CIENCIACTIVA FONDO NACIONAL DE DESARROLLO CIENTIFICO TECNOLOGICO Y DE INNOVACION TECNOLOGICA — Carlos Chois Pimentel — Unidad de Tecnologías de la Información

a. Abarca a toda la información que utiliza el CONCYTEC para el desarrollo de sus actividades, siendo de aplicación y obligatoriedad por el personal interno y externo.

b. Se deben adoptar medidas de seguridad desde el proceso de contratación de personal y hacer de su conocimiento la Política de Seguridad de la Información.

c. Todo personal externo y/o proveedor de servicios relacionado a las tecnologías de información, debe coordinar y/o reportar al Oficial de Seguridad de la Información, las acciones de control a implementar, según corresponda.

CONCYTEC — A. LARREA SÁNCHEZ — OFICINA GENERAL DE ADMINISTRACIÓN

d. Las Oficinas de Personal, Logística o la dependencia equivalente, informarán a su Unidad de Informática el cese o extinción del vínculo contractual con personas naturales, a fin que se proceda al bloqueo que corresponda.

e. Todo el personal interno, externo y/o proveedor de servicio deberán firmar el Compromiso de Confidencialidad o no divulgación que se establezca.

8.3 Seguridad física y entorno:

CONCYTEC — P. VÁSQUEZ — OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

Objetivo: Impedir los accesos no autorizados, daños e interferencia a las Unidades Orgánicas e información de la entidad.

a. El CONCYTEC, deberá establecer una clasificación de los ambientes físicos como público, común ó restringido y de la información a nivel de seguridad.

b. Los recursos de tratamiento de información crítica o sensible para la entidad deberán ubicarse en áreas restringidas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.

CONCYTEC — M. ACUÑA — OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

c. Todo equipo informático que no sea de propiedad del CONCYTEC, debe ser ingresado previo registro de acuerdo al procedimiento que establezca la entidad, de surgir alguna ocurrencia será informado a la Unidad de Informática competente.

d. Todas las visitas de personas externas deben ser consignadas en el registro de visitas, portar el pase de autorización y acceder a las áreas público o común siempre que cuente con autorización del personal de entidad.

CONCYTEC — J. FERNANDEZ — OFICINA GENERAL DE DI ANE

CONCYTEC — V. NARCISO — OFICINA GENERAL DE ASESORÍA JURÍDICA

e. Sólo al personal autorizado le está permitido el acceso a las instalaciones donde se almacena información confidencial, dicho acceso deberá ser solicitado a la Oficina General de Administración o la dependencia equivalente, quien designará la supervisión correspondiente.

f. Los recursos informáticos que se encuentren en el centro de cómputo deberán tener una adecuada instalación, protección eléctrica y mantenimiento, asegurándose que el ambiente en que se encuentran deberá estar protegido contra impactos de desastres como fugas de agua, incendios, etc.

g. La protección física de los equipos informáticos corresponde a quienes en un principio se les asigna, asimismo se deben seguir los procedimientos vigentes para el movimiento de los mismos.

h. Todo el personal del CONCYTEC bajo cualquier modalidad de contratación, será sancionado ante cualquier infracción a la Ley N° 30096, Ley de Delitos Informáticos; o a lo establecido en las políticas, normas y/o procedimientos de la entidad.

8.4 Gestión de comunicaciones y operaciones:

Objetivo: Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información, estos lineamientos deberán.

a. Establecer responsabilidades y procedimientos de gestión y operación para todas las instalaciones; así como efectuar la separación de funciones cuando corresponda.

b. Documentar y mantener los procedimientos de alta criticidad identificados en el sistema de gestión de seguridad de la información. Estos procedimientos, se deberán tratar como documentos formales y sus cambios han de autorizarse por el responsable de dicho procedimiento.

c. Realizar proyecciones de los requisitos futuros de capacidad para reducir el riesgo de sobrecarga del sistema; así mismo se deberá coordinar y revisar regularmente los requisitos de recuperación de caídas de los servicios que soportan aplicaciones múltiples.

d. Utilizar controles y medidas especiales para detectar, evitar y prevenir la introducción de software malicioso. Los usuarios deberán conocer los peligros que puede ocasionar este tipo de amenaza.

e. Implementar una serie de controles y medidas requeridas para conseguir y conservar la seguridad de los datos en las redes de computadores; protegiendo la confidencialidad, autenticidad y disponibilidad de la información.

f. Todo equipo de cómputo de propiedad del CONCYTEC utilizado fuera de la sede y en funciones propias de la entidad, deberá contar con protección igual al de los equipos que se encuentran dentro de las instalaciones.

CONCYTEC - A. LA ROSA SÁNCHEZ - OFICINA GENERAL DE ADMINISTRACIÓN

CONCYTEC - P. VÁSQUEZ - OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

CONCYTEC - M. ACUÑA - OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

CONCYTEC - J. FERNÁNDEZ - OFICINA GENERAL DE PLANEAMIENTO Y PRESUPUESTO

CONCYTEC - A. MANCILLO - OFICINA GENERAL DE ASESORÍA JURÍDICA

CIENCIACTIVA - FONDO NACIONAL DE DESARROLLO CIENTÍFICO TECNOLÓGICO Y DE INNOVACIÓN TECNOLÓGICA - Carlos Chois Pimentel - Unidad de Tecnologías de la Información

g. La entidad vigilará el cumplimiento de los compromisos de seguridad de los servicios de almacenamiento externo, a través de la revisión periódica de los informes de vulnerabilidad entregados a la entidad.

h. Establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos, datos de entrada o salida y documentación del sistema, de daño, robo y acceso no autorizado.

8.5 Control de acceso:

Objetivo: Controlar el acceso a los activos de información e instalaciones de procesamiento sea otorgado en función de las tareas o responsabilidades de cada usuario.

a. Los usuarios con acceso a un sistema informático dispondrán de una única autorización de acceso, compuesta de identificador de usuario y contraseña, y serán los únicos responsables de la confidencialidad de su contraseña y de los cambios que deriven de su uso.

b. Los usuarios tendrán acceso autorizado únicamente a aquellos activos de información que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el director o jefe de cada unidad orgánica.

c. Se deberá contar con técnicas de autenticación y autorización para mantener los niveles de seguridad adecuados.

8.6 Adquisición, desarrollo y mantenimiento de sistemas:

Objetivo: Garantizar la incorporación de medidas de seguridad en los sistemas, aplicativos y portales, desde su desarrollo, implementación y durante su mantenimiento.

a. Diseñar e incluir internamente en cada aplicación las medidas de control e incluir la validación de datos de entrada, el tratamiento interno y los datos de salida; evitando pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.

b. Usar las medidas disponibles de seguridad para proteger la información confidencial; cuando otras medidas y controles no proporcionen la protección adecuada.

c. Asegurar la revisión de todo cambio propuesto a las aplicaciones para comprobar que no debilite su seguridad o la del sistema operativo.

8.7 Gestión de Incidentes:

Objetivo: Asegurar que los incidentes, eventos y debilidades en la seguridad de la información sean comunicados, y se registren de manera que permitan implementar estrategias y acciones correctivas.

a. Todo personal, proveedores de servicios y terceros deben reportar todo tipo de eventos relacionados a la seguridad de la información, sean tecnológicos o no al punto de contacto indicado en los procedimientos relacionados.

CONCYTEC - OFICINA GENERAL DE ADMINISTRACIÓN - A. LA ROSA SÁNCHEZ
CONCYTEC - OFICINA DE TECNOLOGÍAS DE INFORMACIÓN - P. VÁSQUEZ
CONCYTEC - OFICINA DE TECNOLOGÍAS DE INFORMACIÓN - M. ACUÑA
CONCYTEC - OFICINA GENERAL DE ASESORÍA JURÍDICA
CONCYTEC - J. FERNÁNDEZ
CIENCIACTIVA - Carlos Chois Pimentel - Unidad de Tecnologías de la Información

b. El Oficial de Seguridad de la Información en coordinación con las unidades orgánicas involucradas deberán llevar un registro de los incidentes de seguridad ocurridos en su ámbito y alcance, monitoreando la implementación de las acciones correctivas o preventivas que ameriten verificando el procedimiento de respuesta.

c. Todo incidente o evento de seguridad deberá ser registrado por el Sistema de Gestión de la Seguridad de la Información (SGSI), ayudando a identificar cuales son los que más se repiten analizando la causa raíz y la probabilidad de impacto para el CONCYTEC, de acuerdo a los procedimientos que se establezcan

d. El Oficial de Seguridad de la Información debe reportar los incidentes informáticos a la PeCERT según lo señalado en el procedimiento de esta autoridad, así como comunicar los avisos de alerta que envían a esta lista.

8.8 Gestión de continuidad del negocio:

Objetivo: Orientado a contrarrestar las interrupciones de las actividades, proteger los procesos críticos de los efectos de fallas significativas o desastres y asegurar la coordinación con el personal de la entidad y los contactos externos que participarán en las estrategias de planificación de contingencias.

a. Se deberá implantar un proceso de gestión de continuidad de las operaciones para reducir a niveles aceptables, la interrupción causada por desastres y fallas de seguridad mediante una combinación de controles preventivos y de recuperación.

b. Se deberá desarrollar e implementar el Plan de Contingencia Informático de acuerdo a su competencia para la restauración de servicios en el plazo requerido, tras la interrupción de los procesos críticos y asegurar la coordinación con el personal del interno y con los contactos extremos y/o proveedores de servicio que participarán en las estrategias de planificación de contingencias.

8.9 Cumplimiento:

Objetivo: Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

a. Se deberá proteger los registros de información importantes frente al riesgo de pérdida, destrucción y falsificación, y guardar de forma segura ciertos registros, tanto para cumplir determinados requisitos legales o regulatorios, como para soportar actividades esenciales de la entidad.

b. Se deberá proporcionar recursos informáticos exclusivamente para la realización de las actividades laborales. Los Directores y Jefes de las unidades orgánicas deberán autorizar su uso.

c. Se deberá considerar como impropio todo uso de éstos recursos para fines no autorizados o ajenos a las actividades propias de la entidad.

CONCYTEC - A. LA ROSA SÁNCHEZ - OFICINA GENERAL DE ADMINISTRACIÓN

CONCYTEC - P. VÁSQUEZ - OFICINA DE TECNOLOGÍAS DE...

CONCYTEC - N. ACUÑA - OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

CONCYTEC - J. FERNANDEZ - OFICINA GENERAL DE ...

CONCYTEC - ... - OFICINA GENERAL DE ASESORÍA JURÍDICA

CIENCIACTIVA - FONDO NACIONAL DE DESARROLLO CIENTÍFICO, TECNOLÓGICO Y DE INNOVACIÓN TECNOLÓGICA - Carlos Chois Pimentel - Unidad de Tecnologías de la Información

ANEXO A: GLOSARIO DE TÉRMINOS

1. **Activo:** Todo aquello que presenta valor para la institución, tales como: Información; software, físico, como una computadora, intangibles entre otros.
2. **Análisis de riesgos:** Uso sistemático de la información para identificar amenazas e identificar el riesgo.
3. **Confidencialidad**: Garantizar que la información sea accesible únicamente a las personas que cuenten con acceso autorizado.
4. **Disponibilidad**: Garantizar que los usuarios autorizados tengan acceso a información y activos asociados cuando sea necesario.
5. **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una entidad considerando el riesgo.
6. **Incidente de seguridad de la información:** Serie de eventos no deseados que tienen una gran probabilidad de comprometer las operaciones de negocio y de amenazar la seguridad de la Información.
7. **Integridad**: Salvaguardar la exactitud e integridad e la información y activos asociados
8. **Oficial de Seguridad de la Información**: Responsable de impulsar la implementación y cumplimiento de la presente Política en coordinación con el Comité de Gestión de Seguridad de la Información
9. **Propietario de la Información**: Es cualquier persona o entidad a la cual se le asigna la responsabilidad formal de custodiar y asegurar un activo de información o un conjunto de ellos.
10. **Recurso Informático:** Son los equipos de cómputo, los productos de software, los medios magnéticos y la información almacenada en formato digital, susceptibles de ser utilizados por una entidad para llevar adelante sus procesos.
11. **Riesgo:** Combinación de la probabilidad de un evento y sus consecuencias.
12. **Seguridad de la información**: Preservar la integridad, confidencialidad y disponibilidad de la información, además deben involucrarse otras características de autenticidad, responsabilidad, no repudio y fiabilidad.
13. **SGSI:** Es la parte del sistema integral de gestión, basado en el enfoque de riesgo del negocio para establecer, opera, monitorear, revisar, mantener y mejorar la seguridad de la información.
14. **Tecnología de la Información**: Se refiere al conjunto de tecnologías desarrolladas para almacenar, recuperar, transmitir, procesar o administrar los datos que son operados por la entidad o por un tercero para llevar a cabo una función propia de la entidad.

CONCYTEC A. LA ROSA SÁNCHEZ OFICINA GENERAL DE ADMINISTRACIÓN

CONCYTEC P. VÁSQUEZ OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

CONCYTEC M. AGUÑA OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

CONCYTEC J. FERNÁNDEZ OFICINA GENERAL DE ADMINISTRACIÓN

CONCYTEC OFICINA GENERAL DE ASESORÍA JURÍDICA

CIENCIACTIVA FONDO NACIONAL DE DESARROLLO CIENTÍFICO, TECNOLÓGICO Y DE INNOVACIÓN TECNOLÓGICA
Carlos Chois Pimentel
Unidad de Tecnologías de la Información