



RESOLUCION DE PRESIDENCIA No.042 -2008-CONCYTEC-P

Lima, 25 de febrero de 2008

Visto el Memorando N°003-2008-CONCYTEC-OPP por el que se remitió cuatro propuestas de Directivas para su revisión y aprobación; y,

CONSIDERANDO:

Que, el Texto Único Ordenado de la Ley N°28303, Ley Marco de Ciencia, Tecnología e Innovación Tecnológica, establece al CONCYTEC como un organismo público descentralizado adscrito al Sector Educación, con personería jurídica de derecho público interno y autonomía científica, administrativa, económica y financiera;

Que, el CONCYTEC tiene como misión el dirigir, fomentar, coordinar, supervisar y evaluar las acciones de Estado en todo el país en el ámbito de la ciencia, tecnología e innovación tecnológica, orienta las acciones del sector privado, y ejecuta acciones de soporte que impulsen el desarrollo científico y tecnológico del país;

Que, por la Resolución Ministerial N°224-2004-PCM, se estableció el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 1° Edición" en todas las Entidades Integrantes del Sistema Nacional de Informática;

Que, mediante Resolución de Presidencia N° 047 -2006-CONCYTEC-P, se nombró al Comité de Gestión de Seguridad de la Información Institucional del CONCYTEC, encargado de proponer la política de seguridad de la información, así como aquellos procedimientos que permitan que los usuarios utilicen en forma adecuada las herramientas informática disminuyendo el riesgo de pérdida de la información.

Que por Memorando 004-2006-CONCYTEC-CGS, el Presidente del Comité de Gestión de Seguridad elevó a la Alta Dirección del CONCYTEC, la Política de Seguridad de Información del CONCYTEC,

Que, mediante Resolución de Presidencia N° 214 -2006-CONCYTEC-P, se aprobó la Política para Administración de Software de CONCYTEC.

Que, con el propósito de dar cumplimiento a las normas antes citada y a fin de establecer las recomendaciones y usos del correo electrónico, así como de evitar pérdidas de información; mejorar la seguridad de la información; difundir recomendaciones sobre la obtención de copias de respaldo de información que generan y manejan las oficinas; y establecer procedimientos de creación de contraseñas para el acceso a los diferentes servicios y sistemas de información existentes en la institución; es necesario aprobar las directivas correspondientes.

Con el visado del Director de Sistemas de Información y Comunicaciones de CTel, de la Jefa de la Oficina de Planeamiento y Presupuesto, del Jefe de la Oficina de Asesoría Jurídica y del Secretario General (e);



RESOLUCION DE PRESIDENCIA No. 042 -2008-CONCYTEC-P

De conformidad con lo dispuesto por el Texto Único Ordenado de la Ley N° 28303, por la Ley N° 28613; así como por lo dispuesto por el Reglamento de Organización y Funciones del CONCYTEC, aprobado por el Decreto Supremo N° 029-2007-ED;

SE RESUELVE:

ARTICULO ÚNICO.- APROBAR las Directivas Nos. 02, 03, 04 y 05-2008-DSIC, las cuales en Anexos A, B, C, y D forman parte de la presente Resolución de Presidencia, y cuentan con la siguiente denominación:


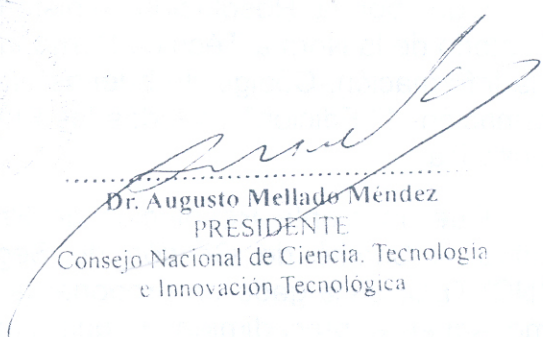
Directiva N° 02-2008-DSIC, Sobre Uso de Correo Electrónico en el CONCYTEC.

Directiva N° 03-2008-DSIC, Procedimiento para Realizar Copias de Respaldo de Información de los Usuarios en el CONCYTEC.

C) Directiva N° 04-2008-DSIC, Sobre Procedimiento de Registro de Incidentes de Seguridad de Información en el CONCYTEC.

D) Directiva N° 05-2008-DSIC, Uso de Contraseñas en el CONCYTEC.

REGÍSTRESE Y COMUNÍQUESE,



Dr. Augusto Mellado Méndez
PRESIDENTE
Consejo Nacional de Ciencia, Tecnología
e Innovación Tecnológica



DIRECTIVA N° 05-2008-DSIC
USO DE CONTRASEÑAS EN EL CONCYTEC

1. ASPECTOS GENERALES

1.1 Finalidad

Normar y establecer los procedimientos y responsabilidades, para la creación, protección, asignación y cambio de las contraseñas de cuentas de los diferentes sistemas y servicios disponibles. La aplicación de la presente directiva se realizará en concordancia con la política de seguridad institucional.

1.2 Objetivos

- 1.2.1 Establecer un procedimiento estándar para la creación de contraseñas en los diferentes servicios y sistemas existentes.
- 1.2.2 Mejorar la confidencialidad de las contraseñas e incrementar la confianza de los usuarios en las mismas.
- 1.2.3 Definir un procedimiento estándar para el cambio de contraseñas que permitan el cambio periódico de las mismas.

1.3 Base Legal

- 1.3.1 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.
- 1.3.2 Ley N° 28613, Ley del Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica.
- 1.3.3 Ley N° 27658 Ley Marco de Modernización de la Gestión del Estado.
- 1.3.4 Resolución Ministerial N°224-2004-PCM del 23 de julio de 2004 - Norma Técnica Peruana "NTP-ISO/IEC 17799:2004 EDI" para uso obligatorio, y sus modificatorias.
- 1.3.5 Reglamento de Organización y Funciones ROF del CONCYTEC, aprobado por Decreto Supremo N° 029-2007-ED.

1.4 Alcance

El ámbito de aplicación de esta directiva incluye a todos los usuarios de los servicios y recursos informáticos del CONCYTEC que tienen o son responsables de una cuenta (o cualquier otro tipo de acceso que requiera una contraseña) en cualquiera de los sistemas.



2 PROCEDIMIENTO PARA CREACION DE CONTRASEÑAS

- 2.1 Para la creación de una cuenta y contraseña en un servicio o sistema, deberá existir el requerimiento del usuario y la aprobación del Jefe o Director de la dependencia correspondiente.
- 2.2 La Dirección de Sistemas de Información y Comunicación de la CTeI - DSIC procederá a crear el "usuario" y contraseña para el servicio o sistema solicitado (considerando las recomendaciones del numeral 5 en cuanto a la contraseña).
- 2.3 El servicio donde el usuario puede cambiar la contraseña una vez creada es el Correo Electrónico. El procedimiento de cambio de contraseñas, se explica en el numeral 4.
- 2.4 Una vez que se entrega el "usuario" y contraseña al usuario, este se hace responsable por su confidencialidad y uso del mismo.

3 PROTECCION DE CONTRASEÑAS

- 3.1 La contraseña es un aspecto fundamental de la seguridad de los recursos informáticos; es la primera línea de protección para el usuario. Una contraseña mal elegida o protegida puede resultar un agujero en la seguridad para toda la organización. Por ello, todos los usuarios de la red del CONCYTEC son responsables de velar por la seguridad de las mismas, las cuales deben seguir las recomendaciones indicadas en el numeral 5.
- 3.2 La seguridad provista por una contraseña depende de que la misma se mantenga siempre en secreto. Todas las directrices suministradas por esta directiva tienen por objetivo mantener esta característica fundamental.
- 3.3- Las contraseñas no deben ser escritas en papel ó incluidas en mensajes de correo electrónico, ni en ningún otro medio de comunicación electrónica. Tampoco deben ser comunicadas en conversaciones telefónicas.
Algunos servicios, en los que sea indispensable el mantener la seguridad de la contraseña, podrán determinar medidas adicionales de protección de la misma.

4 PROCEDIMIENTO PARA EL CAMBIO DE CONTRASEÑAS.

- 4.1 Todas las contraseñas de usuario(cuentas de email, cuentas de acceso a sistemas, cuentas de acceso a red, etc...) deben de ser cambiadas al menos una vez cada 12 meses. Sin embargo, podrá ser cambiada cuando el usuario sospeche que la seguridad de su contraseña puede haber sido comprometida.
- 4.2 El cambio de contraseña se realizará utilizando el instructivo para el cambio de contraseña de cuenta de correo electrónico (Anexo 1).



5 ELECCION DE LA CONTRASEÑA

Todas las contraseñas de cuentas que den acceso a recursos y servicios del CONCYTEC deberán de seguir las siguientes directrices generales:

Las contraseñas deben de tener 8 ó más caracteres y de preferencia que utilice tres caracteres de los cuatro grupos siguientes:

1. Letras minúsculas.
2. Letras mayúsculas.
3. Números (por ejemplo, 1, 2, 3).
4. Símbolos (por ejemplo, ¡, @, Ñ, =, -, etc.).

6 CUMPLIMIENTO

6.1 El incumplimiento de la presente directiva comprometerá la seguridad de la red del CONCYTEC.

6.2 Cada Usuario tendrá la responsabilidad de velar por el cumplimiento de esta directiva así como de su difusión.

6.3 El cumplimiento de la presente directiva podrá ser verificado por la DSIC y por el Órgano de Control Institucional, de acuerdo a lo previsto en su Plan Anual de Control.

6.4 El responsable de cada unidad orgánica, así como el Director de la DSIC, informarán al Comité de Seguridad de la Información Institucional del CONCYTEC, los casos de incumplimiento de la presente Directiva.

6.5 El Comité de Seguridad de la Información del CONCYTEC será el que decida las acciones a tomar en el caso de incumplimiento de la presente directiva una vez establecidas las repercusiones que sobre los recursos y servicios informáticos del CONCYTEC haya podido tener la violación de la misma, sin perjuicio de las acciones disciplinarias, administrativas, civiles o penales que correspondan.

