DIRECTIVA Nº 04-2008-DSIC
SOBRE EL PROCEDIMIENTO DE REGISTRO DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN EN EL CONCYTEC

1. ASPECTOS GENERALES

1.1 Finalidad

Normar y establecer los procedimientos y responsabilidades, para el registro de incidentes de seguridad de información.

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 el registro de incidentes de seguridad de la información.

1.2.2 Mejorar la seguridad de la información en el CONCYTEC.

1.2.3 Generar una base de datos con incidentes de seguridad.

1.3 Base Legal

1.3.1 Texto Único Ordenado de la Ley Nº 28303, Ley Marco de Ciencia, Tecnología e Innovación Tecnológica, aprobado por el Decreto Supremo Nº 032-2007-ED.

1.3.2 Ley Nº 28613, Ley del Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica.

1.3.3 Ley Nº 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 posteriores modificaciones.

1.3.5 Reglamento de Organización y funciones ROF aprobado mediante DS Nro. 029-2007-ED.

1.3.6 Resolución de Presidencia Nº 047-2006-CONCYTEC-P por la que se nombró al Comité de Gestión de Seguridad de la Información Institucional del CONCYTEC

1.4 Alcance

El ámbito de aplicación de esta directiva incluye a todos los usuarios de los servicios y recursos informáticos del CONCYTEC.

1.5 Definición de Incidente de Seguridad

El incidente de seguridad es un evento adverso que compromete o intenta comprometer la confidencialidad, integridad, disponibilidad, legalidad o confiabilidad de la información.

Ciclo de Vida de un Incidente de Seguridad:

2 PROCEDIMIENTO PARA REGISTRO DE INCIDENTES DE SEGURIDAD

2.1 Reportar un incidente de seguridad

Una vez ocurrido un incidente de seguridad, este debe ser comunicado a la brevedad posible al personal de soporte de la Dirección de Sistemas de Información y Comunicación de la CTel - DSIC. El incidente debe registrarse en el formato que se adjunta en el anexo 01 -

2.2 Seguimiento y escalamiento del incidente

a) El incidente deberá ser analizado y clasificado. Se hará una correlación con incidentes anteriores o si es parte de uno mayor, deberá establecerse su origen.

b) En función a la gravedad del problema, se estudiará cuál plan de contingencia se debe aplicar, tomando en cuenta las consecuencias que se pueden generar.

c) Se implementará acciones correctivas siempre y cuando estas sean factibles de realizar.

d) Se mantendrá una comunicación con los afectados ó involucrados en la recuperación del incidente.

e) El incidente se reportará al Comité de Gestión de Seguridad de la Información Institucional, así como las acciones adoptadas.

f) En caso que no se pueda implementar acciones correctivas y se este comprometiendo la seguridad de la información, se comunicará a la Secretaria General.

g) Se deberán implementar medidas preventivas que ayuden a evitar situaciones similares en el futuro.

3 CUMPLIMIENTO

3.1 El incumplimiento de la presente directiva puede llegar a comprometer la seguridad de la información en el CONCYTEC.

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

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

ANEXO 01

Formulario para el Registro de Incidentes de Seguridad

Datos del Reporte

ID	
Fecha y Hora	

Datos del Incidente

Clasificación	
Breve descripción	
Efectos producidos	
Descripción detallada	
Responsable de atención	

Datos del Reportante

Nombre	
Cargo	
Area	
Tel / Anexo	
Email	

Datos Sobre la Solución

Estado	
Fecha de cierre	
Detalle: tareas, tiempos, responsables	