Autorizan ejecución de la "Encuesta de Seguridad de la Información en la Administración Pública - 2010"

RESOLUCIÓN MINISTERIAL N°187-2010-PCM

15 de junio de 2010

CONSIDERANDO:

Que, el artículo 2º del Decreto Supremo N°066-2003-PCM y el numeral 4.8 del artículo 4º y artículo 49° del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por Decreto Supremo N° 063-2007- PCM, disponen que la Presidencia del Consejo de Ministros, a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), actúa como ente rector del Sistema Nacional de Informática, encargándose de normar, coordinar integrar y promover el desarrollo de la actividad informática en la Administración Pública, impulsando el uso de las nuevas tecnologías de la información para la modernización y desarrollo del Estado;

Que, de acuerdo con los numerales 50.1 y 50.3 del artículo 50° del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo N° 063-2007-PCM, son funciones de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), proponer la Estrategia Nacional de Gobierno Electrónico, así como coordinar y supervisar su implementación, realizando acciones orientadas a la consolidación y desarrollo del Sistema Nacional de Informática y supervisar el cumplimiento de la normativa correspondiente;

Que, mediante Resolución Ministerial N° 246-2007-PCM se aprobó 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 las entidades integrantes del Sistema Nacional de Informática;

Que, la Oficina Nacional de Gobierno Electrónico e Informática ha propuesto ejecutar el Reporte de Seguridad de la Información en la Administración Pública -2010, para obtener y mantener actualizada la información técnica relacionada con la seguridad de la información de las entidades del Sistema Nacional de Informática;

De conformidad con lo dispuesto en la Ley N° 29158 - Ley Orgánica del Poder Ejecutivo y el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Decreto Supremo N° 063-2007-PCM y sus modificatorias;

SE RESUELVE:

Artículo 1º.-Autoriza la realización de la "Encuesta ele Seguridad de la Información en la Administración Pública-2010"

Autorizar la ejecución de la "Encuesta de Seguridad de la Información en la Administración Pública - 2010" en todas la entidades de la Administración Pública pertenecientes al Sistema Nacional de Informática.

Artículo 2º.- Aprueba de la "Encuesta de Seguridad de la Información en la Administración Pública - 2010"

Aprobar la "Encuesta de Seguridad de la Información en la Administración Pública - 2010", que como anexo forma parte integrante de la presente Resolución Ministerial.

Artículo 3°,- Publicación

La presente Resolución Ministerial será publicada en el Diario Oficial El Peruano.

La "Encuesta de Seguridad de la Información en la Administración Pública -2010" será publicada en el Portal Institucional de la Presidencia del Consejo de Ministros (www.pcm.gob.pe) y el Portal Institucional de la Oficina Nacional de Gobierno Electrónico e

Informática (ONGEI) (www.ongei.gob.pe), al día siguiente de la publicación de la presente norma en el Diario Oficial "El Peruano".

Artículo 4°.- Plazo

Las entidades de la Administración Pública deberán remitir la Encuesta a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) hasta el 30 de Julio del 2010, de acuerdo a las indicaciones y a la información solicitada en el documento aprobado por el artículo 2° de la presente Resolución Ministerial.

Regístrese, comuníquese y publíquese.

JAVIER VELASQUEZ QUESQUÉN
Presidente del Consejo de Ministros

CUESTIONARIO DE SEGURIDAD DE LA INFORMACION EN LA ADMINISTRACION PUBLICA

PERÚ | Presidencia del Consejo de Ministros | Oficina Nacional de Gobierno Electrónico e Informática

INFORMACION GENERAL	
1. Nombre de la Institución :	
2. Poder, Sector, Gobierno Regional, Gobierno Local u otro pertinente :	
3. Departamento :	
4. Provincia :	
5. Distrito :	
6. Centro Poblado Urbano :	
7. Apellidos y Nombres del Informante :	
8. Teléfono del Informante :	
9. Correo Electrónico del informante :	

(Responder con **X** en la columna Si o No a cada pregunta)

		SI	NO
1.	**Con relación a las Políticas de seguridad de la información**		
a.	¿Se han elaborado políticas de seguridad de la información?		
b.	¿Se están aplicando las políticas de seguridad de la información?		
c.	¿Se hacen de conocimiento al personal de la institución las políticas de seguridad de la información?		
d.	¿Realizan evaluaciones y actualizaciones constantes de las políticas de seguridad de la información?		
e.	¿Las políticas de seguridad de la información están basadas en algún estándar nacional o internacional?		

		SI	NO
2.	**Con relación a la organización para la seguridad de la información**		
a.	¿Tiene la institución un área o una persona asignada para labores exclusivas de seguridad de la información?		
b.	¿El área de seguridad de la información está formalizada dentro del organigrama de la institución?		
c.	¿Tienen un comité de seguridad de la información a nivel de alta dirección?		

d.	¿Tienen asesoramiento especializado en materia de seguridad de la información?		
e.	¿Tienen algún mecanismo de cooperación con organizaciones públicas o privadas referidas a seguridad de la información?		
f.	¿Realizan evaluaciones de seguridad de la información a través de otras entidades públicas o privadas?		
g.	¿Al realizar contratos con empresas externas exige requerimientos de seguridad de la información?		

		SI	NO
3.	**Con relación a la clasificación y control de activos informáticos**		
a.	¿Están clasificados los activos informáticos (hardware, software)?		
b.	¿Cuenta esta clasificación, con un sistema software que la automatice?		
c.	¿Realizan periódicamente la actualización de su inventario de activos informáticos?		
d.	¿Actualizan las etiquetas con nombres de contenidos, fechas, ubicación, versiones y responsables de los activos informáticos?		
4.	**Con relación a las políticas del personal respecto a la seguridad Informática**	**SI**	**NO**
a.	¿Están preparados los usuarios para reportar los incidentes de seguridad de los sistemas de información?		
b.	¿La institución tiene acuerdos con el personal sobre la confidencialidad de la información?		
c.	¿Reciben los usuarios capacitación actualizada en temas de seguridad de la información?		
d.	¿Tienen procedimientos de respuesta a incidentes y anomalías en materia de seguridad informática para ser aplicados por los usuarios?		
e.	¿Los empleados,contratistas y terceros tienen una guía que establezca expectativas de seguridad de su rol?		
5.	**Con relación a la seguridad física y ambiental de los sistemas de Información**	**SI**	**NO**
a.	¿Tienen identificadas las áreas físicas seguras donde se encuentran los sistemas de información?		
b.	¿Tienen controles de ingreso del personal a las áreas físicas donde se encuentran los sistemas de información?		
c.	¿Están preparados para mantener el correcto funcionamiento del suministro eléctrico en caso del alguna falla?		

d.	¿Están preparados para mantener el correcto funcionamiento del cableado de datos en caso del alguna falla?		
e.	¿Tienen mecanismos de seguridad de la información para los equipos que ingresan y salen fuera del ámbito de la institución?		
f.	¿Cuentan con mantenimiento periódico del hardware y software en los equipos informáticos?		
g.	¿Se usan técnicas para que la información de dispositivos de almacenamiento con data sensible no sea recuperable?		
6.	**Con relación a la gestión de las comunicaciones de datos y operaciones de los sistemas informáticos**	**SI**	**NO**
a.	¿Cuentan con procedimientos y responsabilidades operativas del uso y acceso a los sistemas informáticos?		
b.	¿Cuentan con documentación de los procedimientos operativos del uso y acceso de los sistemas informáticos?		
c.	¿Tienen procedimientos para afrontar incidentes de las comunicaciones de datos y operaciones de los sistemas informáticos?		
d.	¿Tienen establecidos controles en la red de datos contra software malicioso (antivirus, antispyware, etc)?		
e.	¿Tienen un registro de acceso y uso de las aplicaciones y servicios de la red de datos del personal operativo?		
f.	¿Tienen un registro de fallas de las comunicaciones de datos?		
g.	¿Tienen un control documentado de toda la información referida a la red de datos, es decir direcciones IP de las maquinas de los usuarios, distribución de las IP, diagrama de la red de datos, entre otros?		
h.	¿Tienen mecanismos de seguridad para proteger la documentación de los sistemas de información?		
i.	¿Tienen establecidos controles de seguridad de los medios de almacenamiento de información en tránsito?		
j.	¿Tienen establecidos controles de seguridad para el sistema de correo electrónico de la institución?		
7.	**Con relación al control de acceso a los sistemas informáticos**	**SI**	**NO**
a.	¿Tienen políticas de control de acceso a los sistemas informáticos de los usuarios en la red de datos?		
b.	¿Se están aplicando las políticas de control de acceso a los sistemas informáticos de los usuarios en la red de datos?		
c.	¿Cuentan con un registro permanente de acceso a los sistemas informáticos de los usuarios en la red de datos?		

d.	¿Cuentan con una administración de los privilegios para acceder a los sistemas informáticos?		
e.	¿Cuentan con una administración de las contraseñas de usuarios para los sistemas informáticos?		
f.	¿Tienen políticas de uso, de los servicios de la red de datos de su institución?		
g.	¿Tienen establecidos mecanismos de autenticación de usuarios para las conexiones externas a la red de datos?		
h.	¿Tienen establecido limitaciones de horario para la conexión a la red de datos?		
i.	¿Están aislados los sistemas informáticos críticos de personal no autorizado?		
j.	¿Tienen mecanismos de monitoreo del uso de los sistemas informáticos?		
k.	¿Tienen controles de seguridad informática de los usuarios que usan computadoras portátiles?		

		SI	NO
8.	**Con relación al desarrollo y mantenimiento de sistemas informáticos**		
a.	¿Realiza el análisis y define especificaciones de los requerimientos de seguridad informática cuando desarrolla sistemas informáticos?		
b.	¿Tienen mecanismos de validación de datos de entrada y de salida los sistemas de información?		
c.	¿Se han establecido controles criptográficos en su red de datos, como por ejemplo el uso de certificados digitales u otros programas para la encriptación de datos?		
d.	¿Tienen políticas de uso de los controles criptográficos en su red de datos?		
e.	¿Tienen servicios de no repudio, es decir que el usuario no pueda negar las acciones realizadas en los sistemas informáticos?		
f.	¿Cuentan con una administración de llaves para los certificados digitales?		
g.	¿Mantienen un control del acceso a los programas fuente de las aplicaciones que utilizan en la red institucional?		
h.	¿Tienen procedimientos de control de los cambios que se realizan en las aplicaciones software y el sistema operativo de los servidores o las estaciones de trabajo?		
i.	¿Realizan revisiones a posibles códigos ocultos maliciosos o código troyano dentro de sus aplicaciones software?		

j.	¿Tienen mecanismos de protección cuando se desarrolla software por parte de personal que no pertenece a la institución?		
9.	**Con relación a la gestión de incidentes de sistemas informáticos**	**SI**	**NO**
a.	¿Realiza algún procedimiento para reportar algún evento o debilidad ?		
b.	¿Usa algún sistema de registro de incidentes o software de Helpdesk?		
c.	¿Realiza la clasificación de incidentes?		
d.	¿Tienen elaborado un plan de respuesta ante incidentes?		
e.	¿Investigan y recolectan evidencias sobre el incidente ?		
f.	¿Evaluan el daño y costo de las incidencias?		
10.	**Con relación a la administración de la continuidad de los sistemas Informáticos**	**SI**	**NO**
a.	¿Tienen elaborado planes de continuidad de las operaciones informáticas?		
b.	¿Están implementados los planes de continuidad de las operaciones informáticas?		
c.	¿Realizan pruebas, mantenimiento y evaluación constante de los planes de continuidad de las operaciones informáticas?		
11.	**Con relación al cumplimiento legal referido a los sistemas Informáticos**	**SI**	**NO**
a.	¿Tienen identificada la normativa legal a la que pueda sujetarse las aplicaciones software que usan en la red de su institución?		
b.	¿Tienen políticas y mecanismos de protección de datos y privacidad de la información del personal de la institución?		
c.	¿Tienen controles de prevención del uso inadecuado de los recursos de procesamiento de información?		
d.	¿Tienen controles del cumplimiento de las políticas de seguridad informática?		
e.	¿Realizan auditoria a los sistemas informáticos de su institución?		

12. Nivel de implementación (marcar con una X)

Politica de Seguridad de la Informacion			Elaboracion de Analisis de Riesgos			Documento de Brecha(implementado y lo que falta implementar)			La implementacion de la Norma se hace con:		Recomendaciones, Sugerencias, Comentarios
No iniciado	Elaborada y en revision	Emitida mediante Normativa	No iniciado	En Proceso	Concluido	No iniciado	En Proceso	Concluido	Personal propio de la institucion	Consultoria contratada	