

	Infraestructura Oficial de Firma	Rev: 03/23-02-2007
	Electrónica IOFE PERU	Aprobado:

ANEXO 4:
CONTROLES DE LOS ESTÁNDARES ISO/IEC 17799,
SECCIONES 5 A 15

CONTROLES DEL ESTÁNDAR ISO/IEC 17799, SECCIONES 5 A 15

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- 5.1 Política de Seguridad de la información
 - 5.1.1 Documentación de la política de seguridad
 - 5.1.2 Revisión y Evaluación

6. ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

- 6.1 Comité de gestión de seguridad de la información
 - 6.1.1 Comité de gestión de seguridad de la información
 - 6.1.2 Coordinación de la seguridad de la información
 - 6.1.3 Asignación de responsabilidades sobre seguridad de información
 - 6.1.4 Proceso de autorización de recursos para el tratamiento de la información
 - 6.1.5 Acuerdos de confidencialidad
 - 6.1.6 Contacto con autoridades
 - 6.1.7 Contacto con grupos de interés especial
 - 6.1.8 Revisión independiente de la seguridad de la información
- 6.2 Seguridad en los accesos de terceras partes
 - 6.2.1 Identificación de riesgos por el acceso de terceros
 - 6.2.2 Requisitos de seguridad cuando sea trata con clientes
 - 6.2.3 Requisitos de seguridad en contratos de outsourcing

7. CLASIFICACIÓN Y CONTROL DE ACTIVOS

- 7.1 Responsabilidad sobre los activos
 - 7.1.1 Inventario de activos
 - 7.1.2 Propiedad de los activos
 - 7.1.3 Uso adecuado de los activos
- 7.2 Clasificación de la información
 - 7.2.1 Guías de clasificación
 - 7.2.2 Marcado y tratamiento de la información

8. SEGURIDAD EN RECURSOS HUMANOS

- 8.1 Seguridad antes del empleo
 - 8.1.1 Inclusión de la seguridad en las responsabilidades y funciones laborales
 - 8.1.2 Selección y política de personal
 - 8.1.3 Acuerdos de confidencialidad
- 8.2 Durante el empleo
 - 8.2.1 Responsabilidades de la gerencia
 - 8.2.2 Conocimiento, educación y entrenamiento de la seguridad de información
 - 8.2.3 Proceso disciplinario
- 8.3 Finalización o cambio del empleo
 - 8.3.1 Responsabilidades de finalización
 - 8.3.2 Retorno de activos
 - 8.3.3 Retiro de los derechos de acceso

9. SEGURIDAD FÍSICA Y DEL ENTORNO

- 9.1 Áreas seguras
 - 9.1.1 Perímetro de seguridad física
 - 9.1.2 Controles físicos de entradas
 - 9.1.3 Seguridad de oficinas, despachos y recursos
 - 9.1.4 Protección contra amenazas externas y ambientales
 - 9.1.5 El trabajo en las áreas seguras
 - 9.1.6 Acceso público, áreas de carga y descarga
- 9.2 Seguridad de los equipos
 - 9.2.1 Instalación y protección de equipos
 - 9.2.2 Suministro eléctrico
 - 9.2.3 Seguridad del cableado
 - 9.2.4 Mantenimiento de equipos
 - 9.2.5 Seguridad de equipos fuera de los locales de la organización
 - 9.2.6 Seguridad en el rehúso o eliminación de equipos
 - 9.2.7 Retiro de la propiedad

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES

- 10.1 Procedimientos y responsabilidades de operación
 - 10.1.1 Documentación de procedimientos operativos
 - 10.1.2 Gestión de Cambios
 - 10.1.3 Segregación de tareas
 - 10.1.4 Separación de los recursos para desarrollo y para producción
- 10.2 Gestión de servicios externos
 - 10.2.1 Servicio de entrega
 - 10.2.2 Monitoreo y revisión de los servicios externos
 - 10.2.3 Gestionando cambios para los servicios externos
- 10.3 Planificación y aceptación del sistema
 - 10.3.1 Planificación de la capacidad
 - 10.3.2 Aceptación del sistema
- 10.4 Protección contra software malicioso
 - 10.4.1 Medidas y controles contra software malicioso
 - 10.4.2 Medidas y controles contra código móvil
- 10.5 Gestión de respaldo y recuperación
 - 10.5.1 Recuperación de la información
- 10.6 Gestión de seguridad en redes
 - 10.6.1 Controles de red
 - 10.6.2 Seguridad en los servicios de redes
- 10.7 Utilización de los medios de información
 - 10.7.1 Gestión de medios removibles
 - 10.7.2 Eliminación de medios
 - 10.7.3 Procedimientos de manipulación de la información
 - 10.7.4 Seguridad de la documentación de sistemas
- 10.8 Intercambio de información
 - 10.8.1 Políticas y procedimientos para el intercambio de información y software
 - 10.8.2 Acuerdos de Intercambio
 - 10.8.3 Medios físicos en tránsito
 - 10.8.4 Seguridad en la mensajería electrónica
 - 10.8.5 Sistemas de Información de Negocios
- 10.9 Servicios de correo electrónico
 - 10.9.1 Comercio Electrónico
 - 10.9.2 Transacciones en línea
 - 10.9.3 Información pública disponible
- 10.10 Monitoreo
 - 10.10.1 Registro de la auditoría
 - 10.10.2 Monitoreando el uso del sistema
 - 10.10.3 Protección de la información de registro
 - 10.10.4 Registro de administradores y operadores
 - 10.10.5 Registro de la avería
 - 10.10.6 Sincronización del reloj

11. CONTROL DE ACCESOS

- 11.1 Requisitos de negocio para el control de accesos
 - 11.1.1 Política de control de accesos
- 11.2 Gestión de acceso de usuarios
 - 11.2.1 Registro de usuarios
 - 11.2.2 Gestión de privilegios
 - 11.2.3 Gestión de contraseñas de usuario
 - 11.2.4 Revisión de los derechos de acceso de los usuarios
- 11.3 Responsabilidades de los usuarios
 - 11.3.1 Uso de contraseñas
 - 11.3.2 Equipo informático de usuario desatendido
 - 11.3.3 Política de pantalla y escritorio limpio
- 11.4 Control de acceso a la red
 - 11.4.1 Política de uso de los servicios de la red
 - 11.4.2 Autenticación de usuario para conexiones externas
 - 11.4.3 Identificación de equipos en las redes
 - 11.4.4 Diagnostico remoto y configuración de protección de puertos
 - 11.4.5 Segregación en las redes
 - 11.4.6 Control de conexión a las redes
 - 11.4.7 Control de enrutamiento en la red
- 11.5 Control de acceso al sistema operativo
 - 11.5.1 Procedimientos de conexión de terminales
 - 11.5.2 Identificación y autenticación del usuario
 - 11.5.3 Sistema de gestión de contraseñas
 - 11.5.4 Utilización de las facilidades del sistema
 - 11.5.5 Desconexión automática de sesiones
 - 11.5.6 Limitación del tiempo de conexión
- 11.6 Control de acceso a las aplicaciones y la información
 - 11.6.1 Restricción de acceso a la información
 - 11.6.2 Aislamiento de sistemas sensibles
- 11.7 Informática móvil y teletrabajo
 - 11.7.1 Informática móvil y comunicaciones
 - 11.7.2 Teletrabajo

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- 12.1 Requisitos de seguridad de los sistemas
 - 12.1.1 Análisis y especificación de los requisitos de seguridad
- 12.2 Seguridad de las aplicaciones del sistema
 - 12.2.1 Validación de los datos de entrada
 - 12.2.2 Control del proceso interno
 - 12.2.3 Integridad de mensajes
 - 12.2.4 Validación de los datos de salida
- 12.3 Controles criptográficos
 - 12.3.1 Política de uso de los controles criptográficos
 - 12.3.2 Gestión de claves
- 12.4 Seguridad de los archivos del sistema
 - 12.4.1 Control del software en producción
 - 12.4.2 Protección de los datos de prueba del sistema
 - 12.4.3 Control de acceso a los códigos de programas fuente
- 12.5 Seguridad en los procesos de desarrollo y soporte
 - 12.5.1 Procedimientos de control de cambios
 - 12.5.2 Revisión técnica de los cambios en el sistema operativo
 - 12.5.3 Restricciones en los cambios a los paquetes de software
 - 12.5.4 Fuga de Información
 - 12.5.5 Desarrollo externo del software
- 12.6 Control de las vulnerabilidades técnicas

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE INFORMACIÓN

- 13.1 Reportando eventos y debilidades de la seguridad de información
 - 13.1.1 Reportando los eventos en la seguridad de información
 - 13.1.2 Reportando debilidades en la seguridad de información
- 13.2 Gestión de las mejoras e incidentes en la seguridad de información
 - 13.2.1 Responsabilidades y procedimientos
 - 13.2.2 Aprendiendo de los incidentes en la seguridad de información
 - 13.2.3 Recolección de evidencia

14. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

- 14.1 Aspectos de la gestión de continuidad del negocio
 - 14.1.1 Incluyendo la seguridad de información en el proceso de gestión de la continuidad del negocio
 - 14.1.2 Continuidad del negocio y evaluación de riesgos
 - 14.1.3 Redacción e implantación de planes de continuidad que incluyen la seguridad de información
 - 14.1.4 Marco de planificación para la continuidad del negocio
 - 14.1.5 Prueba, mantenimiento y reevaluación de los planes de continuidad

15. CUMPLIMIENTO

- 15.1 Cumplimiento con los requisitos legales
 - 15.1.1 Identificación de la legislación aplicable
 - 15.1.2 Derechos de propiedad intelectual (DPI)
 - 15.1.3 Salvaguarda de los registros de la organización
 - 15.1.4 Protección de los datos y de la privacidad de la información personal
 - 15.1.5 Prevención en el mal uso de los recursos de tratamiento de la información
 - 15.1.6 Regulación de los controles criptográficos
- 15.2 Revisiones de la política de seguridad y de la conformidad técnica
 - 15.2.1 Conformidad con la política de seguridad y los estándares
 - 15.2.2 Comprobación de la conformidad técnica
- 15.3 Consideraciones sobre la auditoría de sistemas
 - 15.3.1 Controles de auditoría de sistemas
 - 15.3.2 Protección de las herramientas de auditoría de sistemas