ADMINISTRACION DE CENTROS DE CÓMPUTO

Guía para la presentación de Casos de Estudio: 2018-1

2do. Caso de Estudio: "Centro de Cómputo"

1. Organización
   1.1. Razón social
   1.2. Rubro / Giro de negocios

2. Centro de Cómputo
   2.1. Nombre real del "Centro de Cómputo"

   2.2. Metas y/u Objetivos del "CC"

   2.3. Organigrama de la Organización con indicación de la ubicación del "CC"

   2.4. Estructura del "CC"
      2.4.1. Organigrama de puestos de trabajo
      o
      Estructura funcional por Unidades o Áreas del CC
      + Funciones de cada área ó unidad
      2.4.2. Personal:
      – Nombre de la plaza, puesto ó cargo
      + Funciones de la plaza, puesto ó cargo
      + Perfil profesional

   2.5. Hardware
      2.5.1. Equipos convencionales:
      – PC's, Laptops, Servidores, impresoras, impresoras de red, equipos multifuncionales, ...
      2.5.2. Red:
      Dispositivos de red: switches, routers, hubs, AP's,...
      Cableado de backbone: tipo, velocidad
      Cableado horizontal: tipo, categoría, velocidad, certificación, etc.
      2.5.3. Dispositivos de seguridad, de protección, y otros equipos:
      – Firewall, UPS, Sistemas de vigilancia,...
      – Otros equipos: equipos de refrigeración,...

   2.6. Software
      2.6.1. Sistema Operativo de desktop
      (Para c/ítem indicar nombre, versión)
      2.6.2. Software de oficina y Aplicativos especializados
      Software propietario comercial y/o especializado de desktop
      + Software libre especializado de desktop (si lo hubiera)
      (Para c/ítem indicar nombre, versión)
      2.6.3. Software de seguridad (antivirus, anti-spam, etc.)
      2.6.4. Sistema Operativo de red, Software para servidores: de archivos, de aplicaciones, web, de correo, DNS, de BDs, de telefonía IP, etc.
      (Para c/ítem indicar nombre y versión del SO de red y/o de la aplicación servidor)

2.6.5. Desarrollo propio (si ese fuera el caso)
- Herramienta(s) de desarrollo
- Metodología(s) de desarrollo
- SI's ó aplicaciones desarrolladas ó en desarrollo

2.6.6. Aplicaciones que el "CC" no supervisa (si los hubiera)
2.6.7. Licenciamiento y/o Outsourcing

2.7. Políticas de Seguridad (relacionadas con TI)
2.7.1. Políticas de seguridad de alto-nivel / Políticas de seguridad de nivel empresarial
(Ejemplos: metas – direcciones estratégicas organizacionales para la seguridad – asignación de recursos para la implementación de la seguridad – asignación de responsabilidades – etc.)
2.7.2. Políticas de seguridad para temas/asuntos específicos
(Ejemplos: el enfoque para la gestión del riesgo y para el plan de contingencias – la protección de la información confidencial/propietaria – el software no autorizado – el cifrado de archivos – traer otros medios de almacenamiento al centro de trabajo – uso de las redes corporativas y el Internet – uso de fax y teléfono – uso del correo electrónico – etc.).
2.7.3. Políticas de seguridad para sistemas específicos (SI's, SO's)
(Ejemplos: solo las personas del departamento de Personal están autorizadas para proporcionar ó modificar información usada en el procesamiento de las planillas – ningún empleado puede actualizar sus propios registros de planillas – listas de control de acceso (ACL's) – tablas de capacidad/directivas de seguridad del SO – reglas de configuración relacionadas con las seguridad de los sistemas – etc.).

ó

2.7.1. Políticas de control del acceso
+ Políticas para el acceso a redes y servicios de red
2.7.2. Políticas de copias de respaldo, copias de seguridad, o backups
2.7.3. Políticas para el desarrollo seguro de software y de sistemas
2.7.4. Políticas de escritorio "despejado" y de pantalla "desbloqueada"
2.7.5. Políticas sobre tipos de software que los usuarios pueden instalar
2.7.6. Políticas para la transferencia de información dentro de la organización y con cualquier entidad externa.
2.7.7. Políticas sobre el uso de controles criptográficos
2.7.8. Políticas para los dispositivos móviles (y uso del "teleworking")
2.7.9. Políticas de seguridad de la información para la inter relación con proveedores

2.8. Plan de Contingencias
2.8.1. Objetivos
2.8.2. Alcance
2.8.3. Responsabilidad
2.8.4. Medidas
(Acciones generales iniciales a tomar para limitar el daño, el perjuicio, o la pérdida, y para proteger las vidas. Pasos generales a ser tomados para brindar soporte para las funciones críticas y/o para lograr la continuidad del negocio, etc.).

2.8.5. Gestión del Riesgo

– Identificación del Riesgo (amenazas, …)
(Lista de riesgos (amenazas, ...) identificados)
– Análisis del Riesgo – Evaluación del Riesgo
(Proponer una evaluación inicial realista del riesgo según la siguiente tabla)

Tabla de Análisis – Evaluación del Riesgo:

# de prioridad	Riesgo	Probabilidad (de ocurrencia)	Impacto	Exposición al Riesgo = probabilidad x impacto

Usar las tablas de impacto y de ocurrencia de las diapositivas del curso, y ORDENAR la TABLA de la MAYOR EXPOSICIÓN a la MENOR EXPOSICIÓN)

– Tratamiento del Riesgo / Control del Riesgo:
(Solo una lista de acciones/estrategias generales realistas/pragmáticas para tratar/controlar/minimizar los riesgos identificados en el paso anterior)

2.8.6. Plan de Recuperación ante eventos perjudiciales (incidentes, desastres, …)
Para cada evento perjudicial previsto desarrollar DETALLADAMENTE lo siguiente:
– Nombre dado al evento perjudicial
+ Probabilidad de ocurrencia del evento perjudicial
+ Severidad del evento perjudicial
+ Recursos y/o Acciones previas al evento perjudicial
+ Acciones durante el evento perjudicial
+ (Si dable) Acciones después del evento perjudicial

2.8.7. Anexo(s)
(Puede ser el Glosario de términos)

2.9. Plan Operativo en TIC / Plan Operativo Informático - (2018)
(Esquema a seguir):
– Período del plan
(Tiene que corresponder al año actual)
– Situación actual
. FODA
. ...
– Alineamiento con el Plan Estratégico Institucional
+ Objetivos Institucionales (relacionados con la actividad informática)
+ Objetivos específicos informáticos (del CC o Departamento de TI)
– Estrategias para el logro de las metas del Plan Operativo Informático
(Listado de acciones generales para el logro de las metas del POI)

– Programación/Relación de Actividades y/o Proyectos Informáticos del POI
+ Gestión de la actividad, y/o proyecto, y asignación de recursos:
. Responsable principal ó líder de la actividad, y/o proyecto

. Descripción de la actividad, y/o proyecto
. Recursos asignados (personal, equipos, dinero,...)
. Fecha prevista de conclusión de la actividad, y/o proyecto, y/o de la entrega de la salida esperada

(Nota: los planes de años anteriores se calificarán con la nota de 0)

2.10. presupuesto asignado al CC.

Notas para el C/E 2:

- Todos los temas son necesarios.
- Los temas de Políticas de seguridad, Plan de Contingencias y Plan Operativo tienen ponderación alta.
- No debe ser de una organización (empresa, institución, firma comercial, etc.) que esté en la lista negra.
- El grupo deberá ASUMIR una POSICIÓN CRÍTICA sobre el CC presentado.
- Para el Plan Operativo en TIC o Informático, EL GRUPO DEBERÁ ENTREGAR EL DOCUMENTO FUENTE UTILIZADO, el cual sin lugar a dudas deberá corresponder al año exigido en esta guía, caso contrario todo el tema de Plan Operativo será calificado con 0.
- El grupo deberá preparar una presentación COMPLETA del caso de estudio en diapositivas.

Lista Negra:

2015-2:
CORPAC S.A. (Corporación Peruana de Aeropuertos y Aviación Comercial S.A.)
MUNICIPALIDAD DISTRITAL DE SAN JERÓNIMO – Cusco
Programa Nacional de Becas y Crédito (PRONABEC), (BECA 18)
OSIPTEL (Organismo Supervisor de Inversión Privada en Telecomunicaciones)
;
2016-1:
Municipalidad Distrital de Santa Anita
Empresa Municipal de Agua Potable y Alcantarillado de Coronel Portillo
INSTITUTO PERUANO DE ENERGIA NUCLEAR
;
2016-2:
Despacho Presidencial – Perú
Ministerio del Ambiente (MINAM) – Perú
Organismo supervisor de las Contrataciones del Estado – OSCE – Perú
;
2017-1:
Ministerio de Desarrollo e Inclusión Social (MIDIS) – Perú
Ministerio de la Producción – Perú
MUNICIPALIDAD PROVINCIAL DE CHICLAYO
;
2017-2:
Presidencia del Consejo de Ministros (PCM)
INSTITUTO DEL MAR DEL PERÚ - IMARPE
Hospital Dos de Mayo