

2.3. Evaluar la importancia del sistema informático en los procesos principales del negocio. Para cada actividad:

- en que porcentaje están las ventas controladas por el sistema informático.
- En que porcentaje esta la administración controladas por el sistema informático.
- En que porcentaje esta la producción controlada por el sistema informático.

Actividad	Ventas %	Administración %	Producción %

2.4 Evaluar el factor de control para medir cada actividad. Muchas veces la mayoría de los trabajos que contribuyen al margen bruto pueden seguir siendo llevados a cabo en parte, aún cuando haya interrupción de sistemas (actividades de diseño, comercial, organización, investigación).

Este factor de control mide el porcentaje del margen bruto que está relacionado directamente al proceso de sistemas.

Actividad	Factor de Control en %	Comentarios

2.5. Cuales son las aplicaciones críticas y/o sistemas cuyo fallo o interrupción afectaría seriamente sus relaciones comerciales, sus ingresos y su imagen? (puede ser un sistema de utilización propio o ajeno)

2.6. Evaluar el periodo de apagón que tendría un impacto significativo en su negocio

Actividad	Periodo máximo de interrupcion antes de afectar la actividad					
	Inmediatamente	> 12 h	> 24 h	> 48 h	> 72 h	> 5 días
	Inmediatamente	> 12 h	> 24 h	> 48 h	> 72 h	> 5 días
	Inmediatamente	> 12 h	> 24 h	> 48 h	> 72 h	> 5 días
	Inmediatamente	> 12 h	> 24 h	> 48 h	> 72 h	> 5 días
	Inmediatamente	> 12 h	> 24 h	> 48 h	> 72 h	> 5 días
	Inmediatamente	> 12 h	> 24 h	> 48 h	> 72 h	> 5 días
	Inmediatamente	> 12 h	> 24 h	> 48 h	> 72 h	> 5 días
	Inmediatamente	> 12 h	> 24 h	> 48 h	> 72 h	> 5 días

3. Plan de continuidad del negocio:

3.1. Comentario sobre si hay un plan de recobro/reanudación para evitar el cese de negocio debido al fallo del sistema, a través de planes de contingencia y/o procedimientos internos alternativos (interdependencia, cambios en el proceso, gastos adicionales, etc.)

3.2. Evaluar el porcentaje de facturación, normalmente controlada por la aplicación interrumpida, y que puede ser mantenida por medidas alternativas.

Existe esta posibilidad para evitar perdidas importantes de beneficio gracias a unos planes de contingencia y/o introduciendo procedimientos de trabajo alternativos. A menudo se puede reducir la interrupción del negocio a través de:

- La subcontratación de tareas no cumplidas a terceros (planes de continuidad, etc)
- Cambios en el proceso (pedidos por fax y teléfono reemplazando EDI o e-business)
- Incurriendo en gastos adicionales de contratación como recursos temporales, etc.

Actividad	Factor de Contingencia en %	Comentarios

4. Medidas de seguridad informática

Para los siguientes 7 criterios, señalar el nivel de seguridad para cada uno.

Protección física	
	<i>Nivel 0.</i> Ninguna medida específica
	<i>Nivel 1.</i> Detector de incendios en áreas críticas
	<i>Nivel 2:</i> nivel 1 + alarma está conectada a un central de 24 horas
	<i>Nivel 3:</i> nivel 2 + sistema de extinción automático de incendios
	<i>Nivel 4:</i> nivel 3 + mantenimiento y comprobación periódica

Gestión de "back-ups"	
	<i>Nivel 0.</i> Ninguna medida específica
	<i>Nivel 1.</i> Control semanal, al menos.
	<i>Nivel 2:</i> nivel 1 + operación diaria de "backup"
	<i>Nivel 3:</i> nivel 2 + almacenamiento semanal afuera de los locales de la oficina
	<i>Nivel 4:</i> nivel 3 + pruebas de restauración o uso efectivo

Organización	
	<i>Nivel 0.</i> Ninguna medida específica
	<i>Nivel 1.</i> Directrices escritas (totalmente o parcialmente)
	<i>Nivel 2:</i> nivel 1 + política de seguridad por escrito
	<i>Nivel 3:</i> nivel 2 + Responsable de seguridad de la información o función identificada
	<i>Nivel 4:</i> nivel 3 + Auditoría periódica con compromisos específicos obligatorios

Detección de Intrusión	
	<i>Nivel 0.</i> Ninguna medida específica
	<i>Nivel 1.</i> Hay firewall arquitectura
	<i>Nivel 2:</i> nivel 1 + instrumentos de supervisión
	<i>Nivel 3:</i> nivel 2 + mantenimiento y pruebas periódicas
	<i>Nivel 4:</i> nivel 3 + equipo para solucionar incidencias 24h/día

Control del Acceso Interno	
	<i>Nivel 0.</i> Ninguna medida específica
	<i>Nivel 1.</i> Contraseña individual obligatoria
	<i>Nivel 2:</i> nivel 1 + los perfiles y derechos privilegios la dirección
	<i>Nivel 3:</i> nivel 2 + gestión del contraseña (e.g. validación)
	<i>Nivel 4:</i> nivel 3 + procedimiento formalizado (p. ej. administración, revocación)

Protección anti-Virus	
	<i>Nivel 0.</i> Uso limitado
	<i>Nivel 1.</i> Todos los puestos de trabajo, servidores y entradas tienen sistema antivirus instalados
	<i>Nivel 2:</i> nivel 1 + al menos una actualización semanal
	<i>Nivel 3:</i> nivel 2 + arquitectura distribuida que permite una actualización antivirus automática de los equipos
	<i>Nivel 4:</i> nivel 3 + solución totalmente probada, alerta de la evaluación y equipo de respuesta de incidente, 24 horas / 7 días, con autorización para tomar todas las medidas necesarias

Plan de contingencia del negocio	
	<i>Nivel 0.</i> Ninguna medida específica
	<i>Nivel 1.</i> Plan actualizado para reemplazar equipo crítico de IT dañado
	<i>Nivel 2 :</i> Plan actualizado para reemplazar todo el equipo dañado de IT
	<i>Nivel 3:</i> nivel 2 + disponibilidad de recursos (e.g. local de contingencia)
	<i>Nivel 4:</i> nivel 3 + plan de pruebas periódicas y actualizaciones

5. Facilitar su mejor estimación del total del presupuesto de Sistema de Información

Ha hecho recientemente una auditoria de seguridad IT? Si No
Si la respuesta es si, quien y cuando se hizo?

Este cuestionario ha sido cumplimentado por:

Nombre _____

Fecha _____

Cargo _____

Firma _____