



Universidad de Santiago de Chile
Facultad de Ingeniería
Departamento de Informática

Gestión y Gobernanza TI

Entregar, Dar Servicio y Soporte

Luis Berríos P.
1er Semestre 2025



CONTENIDOS

- Introducción al Dominio de Gestión Entregar, Dar Servicio y Soporte.
- Gestionar las operaciones.
- Gestionar las peticiones y los incidentes de servicio.
- Gestionar los problemas.
- Gestionar la continuidad.
- Gestionar los servicios de seguridad.
- Gestionar los controles de procesos de negocio.
- Resumen.





Universidad de Santiago de Chile
Facultad de Ingeniería
Departamento de Informática

Gestión y Gobernanza TI

Introducción al Dominio de Gestión
Entregar, Dar Servicio y Soporte



Introducción al Dominio de Gestión Entregar, Dar Servicio y Soporte

Introducción

- DSS – Deliver, Service and Support.
- Dominio de Gestión que aborda la entrega operativa y el soporte de los servicios de información y tecnología (I&T), incluida la seguridad.

DSS01—Gestionar
las operaciones

DSS02—Gestionar
las solicitudes
e incidentes
de servicio

DSS03—Gestionar
los problemas

DSS04—Gestionar
la continuidad

DSS05—Gestionar
los servicios
de seguridad

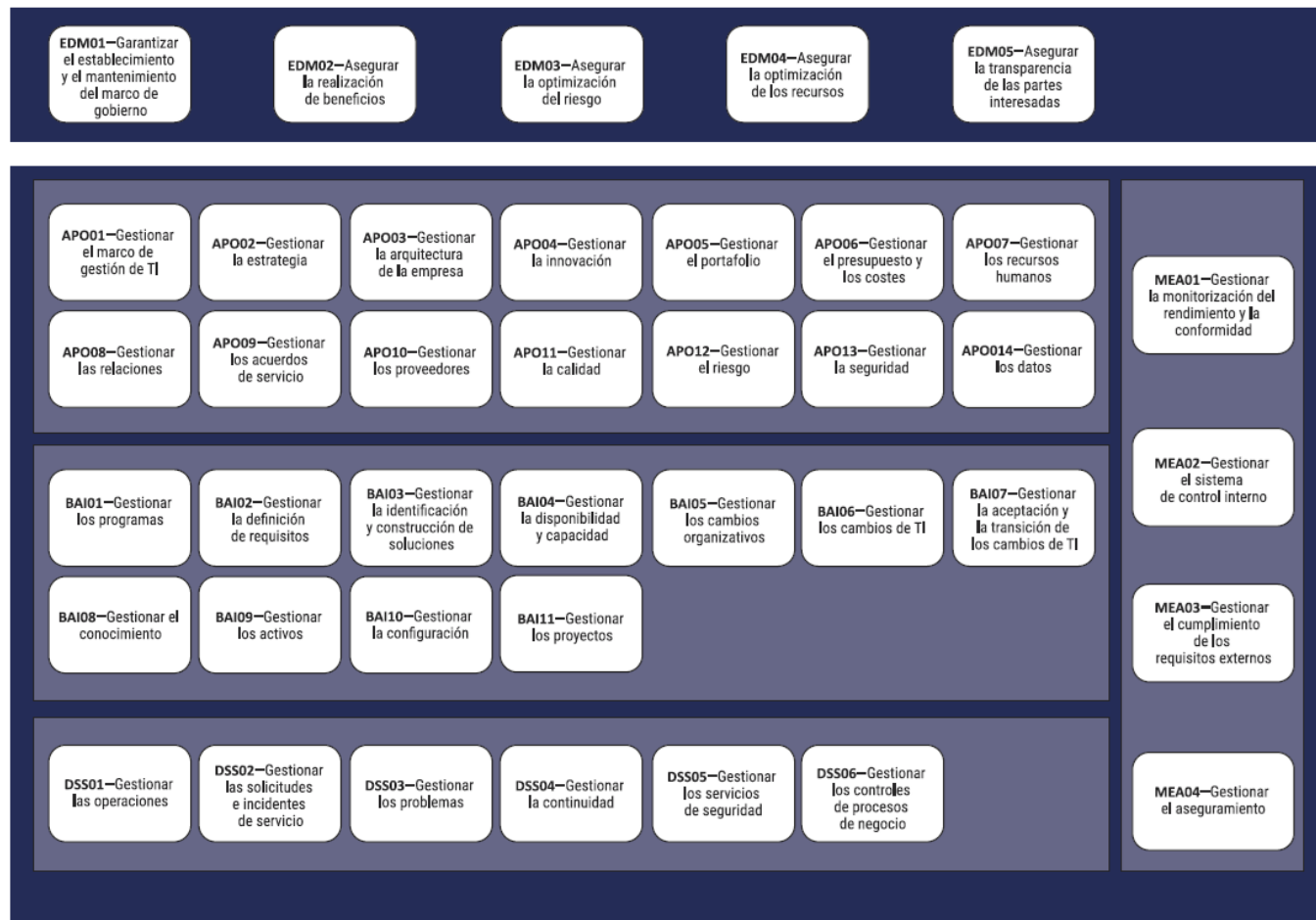
DSS06—Gestionar
los controles
de procesos
de negocio



Introducción al Dominio de Gestión

Entregar, Dar Servicio y Soporte

Introducción

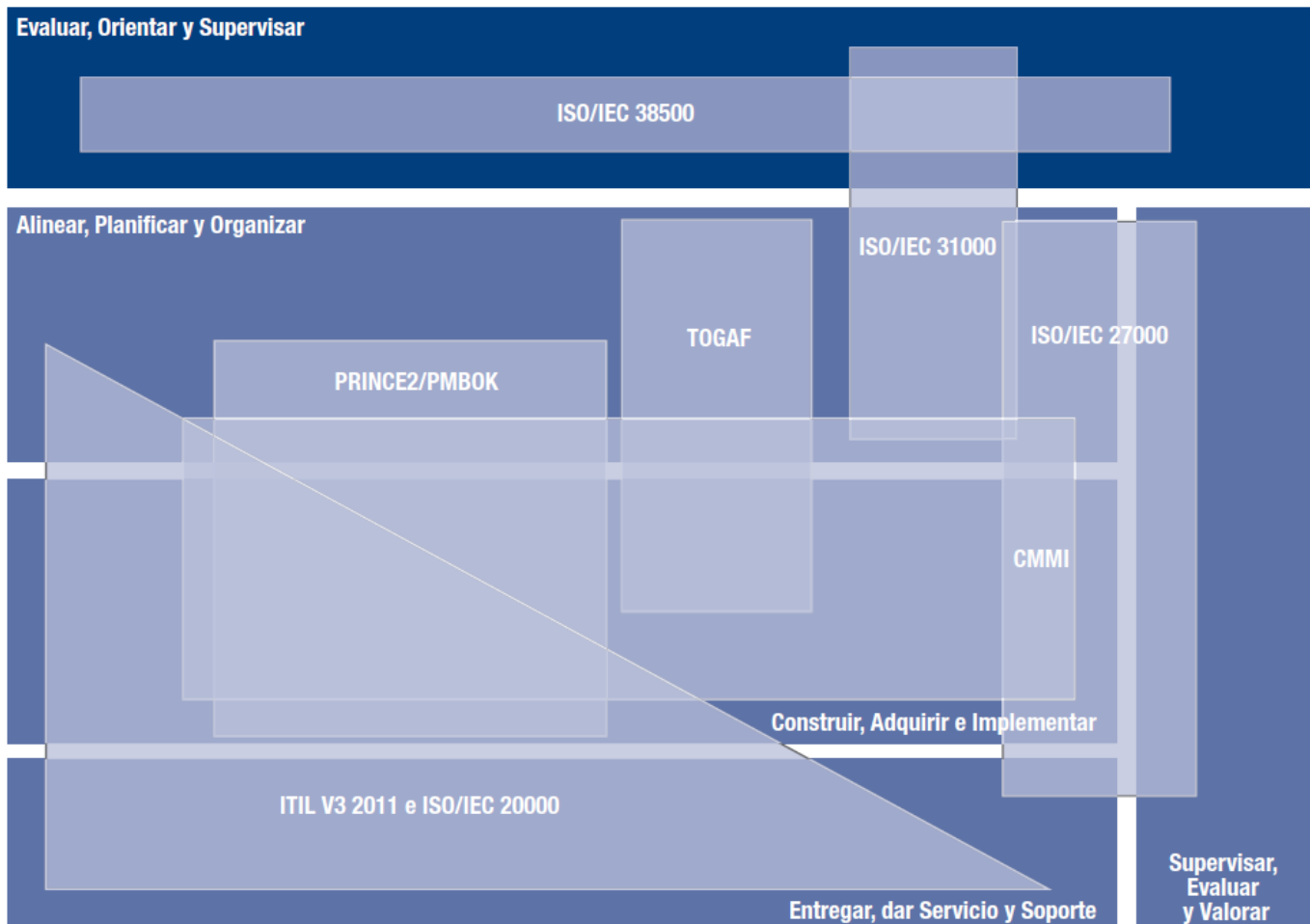


Entregar, Dar Servicio y Soporte (DSS – Deliver, Service and Support)



Introducción al Dominio de Gestión Entregar, Dar Servicio y Soporte

Introducción





Universidad de Santiago de Chile
Facultad de Ingeniería
Departamento de Informática

Gestión y Gobernanza TI

Gestionar las Operaciones



Gestionar las Operaciones

Introducción

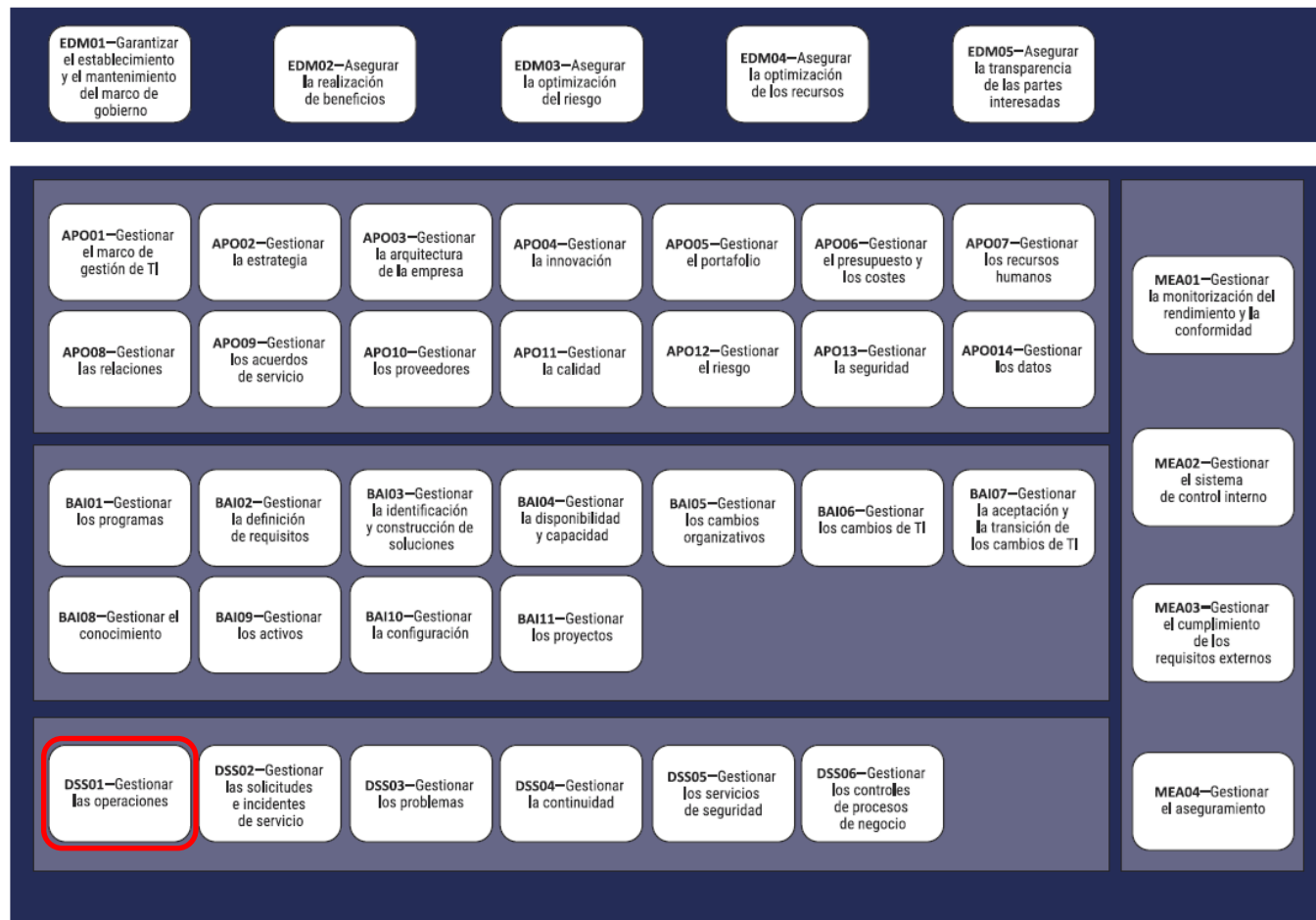
- DSS01 – Gestionar las operaciones.
- Pertenece al Dominio de Gestión Entregar, Dar Servicio y Soporte (DSS – Deliver, Service and Support).





Gestionar las Operaciones

Introducción



Entregar, Dar Servicio y Soporte (DSS – Deliver, Service and Support)



Gestionar las Operaciones

Descripción

- Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar los servicios de I&T, internos y externalizados.
- Incluir la ejecución de procedimientos de operación estándar predefinidos y las actividades de supervisión requeridas.





Gestionar las Operaciones

Propósito

- Proporcionar los resultados de los productos y servicios operativos de I&T según lo planeado.





Gestionar las Operaciones

Componentes


- Procesos (5):
 - DSS01.01 Ejecutar procedimientos operativos.
 - DSS01.02 Gestionar servicios tercerizados de I&T.
 - DSS01.03 Monitorizar la infraestructura de I&T.
 - DSS01.04 Gestionar el medioambiente.
 - DSS01.05 Gestionar las instalaciones.
- Estructuras organizativas.
- Flujos y elementos de información.
- Personas, habilidades y competencias (6).
- Políticas y procedimientos (1).
- Cultura, ética y comportamiento (1).
- Servicios, infraestructura y aplicaciones (3).





Gestionar las Operaciones

El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:

Metas Empresariales			Metas de Alineamiento	
<ul style="list-style-type: none">EG01 – Portafolio de productos y servicios competitivosEG08 – Optimización de la funcionalidad de procesos del negocio internos			<ul style="list-style-type: none">AG05 – Prestación de servicios de I&T conforme a los requisitos del negocio	
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento	
EG01	<ul style="list-style-type: none">Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercadoPorcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del clientePorcentaje de productos y servicios que proporcionan una ventaja competitivaPlazo de comercialización para nuevos productos y servicios		AG05	<ul style="list-style-type: none">Porcentaje de partes interesadas del negocio satisfechas con la prestación de servicios de I&T que cumple con los niveles de servicio acordadosNúmero de interrupciones del negocio debido a incidentes de servicios de I&TPorcentaje de usuarios satisfechos con la calidad de la prestación de servicios de I&T
EG08	<ul style="list-style-type: none">Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarialNiveles de satisfacción de los clientes con las capacidades de prestación de serviciosNiveles de satisfacción de los proveedores con las capacidades de la cadena de suministro			



Gestionar las Operaciones

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS01.01 Ejecutar procedimientos operativos Mantener y ejecutar procedimientos y tareas operativas de manera confiable y consistente.	<ul style="list-style-type: none">Número de incidentes causados por problemas operativosNúmero de procedimientos operativos no estándar ejecutados	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">Desarrollar y mantener los procedimientos operativos y las actividades relacionadas para respaldar todos los servicios prestados.		2
<ul style="list-style-type: none">Mantener un calendario de las actividades operativas y ejecutar las actividades.		3
<ul style="list-style-type: none">Comprobar que todos los datos esperados para su procesamiento se reciban y procesen de forma completa, precisa y en el plazo debido.Entregar el producto conforme a los requisitos de la empresa.Soportar las necesidades de reinicios y reprocesamientos.Asegurar que los usuarios reciban los productos adecuados de forma segura y en el plazo debido.		
<ul style="list-style-type: none">Gestionar el rendimiento y throughput (velocidad a la que se transmiten los datos) de las actividades programadas.		
<ul style="list-style-type: none">Monitorizar los incidentes y problemas relacionados con los procedimientos operativos y realizar las acciones adecuadas para mejorar la confiabilidad de las tareas operativas ejecutadas.		5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		TP.SE Safeguard Operational Environment
HITRUST CSF versión 9, septiembre de 2017		09.01 Document Operating Procedures
ISO/IEC 27002:2013/Cor.2:2015(E)		12.1 Operational procedures and responsibilities
ITIL V3, 2011		Service Operation, 4.1 Event Management
National Institute of Standards and Technology Special Publication 800–53, Revisión 5 (Borrador), agosto de 2017		3.13 Physical and environmental protection (PE–13, PE–14, PE–15)



Gestionar las Operaciones

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS01.02 Gestionar servicios tercerizados de I&T Gestionar la operación de los servicios tercerizados de I&T para mantener la protección de la información empresarial y la confiabilidad de la provisión del servicio.	<ul style="list-style-type: none">Número de KPI específicos/SMART incluidos en los contratos de externalizaciónFrecuencia de falla del socio subcontratista para cumplir con los KPI	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">Asegurar que los requisitos de los procesos de seguridad de la información de la empresa cumplan con los contratos y SLA de hosting de terceros o proveedores de servicios.		3
<ul style="list-style-type: none">Asegurar que los requisitos de procesamiento operacional del negocio y de TI de la empresa y las prioridades para la prestación de servicios cumplan con los contratos y SLA de hosting de terceros o proveedores de servicios.		
<ul style="list-style-type: none">Integrar los procesos de gestión de TI internos críticos con los de los proveedores de servicios externalizados. Esto debería cubrir, por ejemplo, la planificación de rendimiento y capacidad, gestión del cambio, gestión de la configuración, solicitud de servicios y gestión de incidentes, gestión de problemas, gestión de la seguridad, continuidad del negocio y monitorización del rendimiento y reporte del proceso.		
<ul style="list-style-type: none">Planificar una auditoría independiente y el aseguramiento de los entornos operacionales de proveedores que proporcionen servicios externalizados para confirmar que se han abordado de forma adecuada los requisitos acordados.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
ISF, The Standard of Good Practice for Information Security 2016	SC1.2 Outsourcing	
ISO/IEC 20000–1:2011(E)	4.2 Governance of processes operated by other parties	



Gestionar las Operaciones

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS01.03 Monitorizar la infraestructura de I&T <ul style="list-style-type: none">Monitorizar la infraestructura de I&T y eventos relacionados.Almacenar suficiente información cronológica en los logs de operación que permita la reconstrucción y revisión de las secuencias temporales de las operaciones y otras actividades asociadas o que apoyan las operaciones.	<ul style="list-style-type: none">Porcentaje de tipos de eventos operativos críticos cubiertos por sistemas de detección automáticaPorcentaje de activos de infraestructura monitorizados conforme a la criticidad del servicio y la relación entre los elementos de configuración y servicios que dependen de ellos	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">Registrar los eventos.Identificar el nivel de información que debe registrarse, conforme a una consideración de riesgo y rendimiento.		2
<ul style="list-style-type: none">Identificar y mantener una lista de activos de infraestructura que deben monitorizarse conforme a la criticidad del servicio y la relación entre los elementos de configuración y servicios que dependen de ellos		3
<ul style="list-style-type: none">Definir e implementar reglas que identifiquen y registren incumplimientos de umbrales y los estados de eventos.Encontrar un equilibrio entre la generación de eventos menores insignificantes y eventos significativos para que los registros de eventos no estén sobrecargados de información innecesaria.		
<ul style="list-style-type: none">Producir registros de eventos y conservarlos durante un periodo de tiempo adecuado para que ayuden en futuras investigaciones.Garantizar que se creen tickets de incidentes en el plazo debido a la hora de monitorizar desviaciones identificadas en los umbrales definidos.		
<ul style="list-style-type: none">Establecer procedimientos para monitorizar los registros de eventos.Llevar a cabo revisiones regulares.		4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
National Institute of Standards and Technology Special Publication 800–53, Revisión 5 (Borrador), agosto de 2017		3.10 Maintenance (MA–2, MA–3)



Gestionar las Operaciones

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS01.04 Gestionar el medioambiente <ul style="list-style-type: none">Mantener medidas de protección contra los factores medioambientales.Instalar equipos y dispositivos especializados para monitorizar y controlar el ambiente.	<ul style="list-style-type: none">Número de personas capacitadas para responder a los procedimientos de alarma medioambientalNúmero de escenarios de riesgo definidos para las amenazas medioambientales	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">Identificar los desastres naturales y causados por el hombre que podrían ocurrir en el área en la que se encuentran las instalaciones de TI.Evaluar el efecto potencial en las instalaciones de TI.		2
<ul style="list-style-type: none">Identificar cómo el equipo de I&T, incluido el equipo móvil y el off–site, se protege de las amenazas medioambientales.Asegurar que la política limita o excluye el consumo de comida, bebida y fumar en áreas sensibles, y prohibir el almacenamiento de artículos de papelería y otros suministros que suponen un peligro de incendio en las salas de ordenadores.		
<ul style="list-style-type: none">Mantener los centros de TI y salas de servidores limpios y seguros en todo momento (es decir, sin desorden, papel, cajas de cartón, papeleras llenas, productos químicos o materiales inflamables).		
<ul style="list-style-type: none">Situar y construir las instalaciones de TI para minimizar y mitigar la susceptibilidad a las amenazas medioambientales (ej. robo, aire, incendio, humo, agua, vibración, terrorismo, vandalismo, químicos, explosivos).Considerar zonas de seguridad y/o células ignífugas específicas (ej. ubicar los entornos/servidores de producción y desarrollo apartado uno del otro).		3
<ul style="list-style-type: none">Comparar las medidas y planes de contingencia con los requisitos de las políticas de seguros y los resultados del informe.Abordar los puntos de incumplimiento en el plazo debido.		
<ul style="list-style-type: none">Responder a las alarmas medioambientales y a otras notificaciones.Documentar y probar los procedimientos, lo cual debería incluir la priorización de alarmas y contacto con las autoridades de respuesta a emergencia locales.Capacitar al personal en estos procedimientos.		



Gestionar las Operaciones

Componente: Procesos

Práctica de Gestión		Métricas Modelo	
DSS01.04 Gestionar el medioambiente <ul style="list-style-type: none">Mantener medidas de protección contra los factores medioambientales.Instalar equipos y dispositivos especializados para monitorizar y controlar el ambiente.		<ul style="list-style-type: none">Número de personas capacitadas para responder a los procedimientos de alarma medioambientalNúmero de escenarios de riesgo definidos para las amenazas medioambientales	
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">Monitorizar y mantener regularmente dispositivos que detecten proactivamente amenazas medioambientales (ej. fuego, agua, humo, humedad).			4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
National Institute of Standards and Technology Special Publication 800–37, Revisión 2 (Borrador), mayo de 2018		2.1 System and system elements; 3.2 Categorization (Task 5, 6)	



Gestionar las Operaciones

Componente: Procesos

Práctica de Gestión	Métricas Modelo
DSS01.05 Gestionar las instalaciones. Gestionar las instalaciones, incluidos los equipos de suministro eléctrico y comunicaciones, alineados con las leyes y reglamentos existentes, los requisitos técnicos y del negocio, las especificaciones del proveedor, y las directrices de salud y seguridad.	<ul style="list-style-type: none">• Tiempo transcurrido desde la última prueba del suministro de energía ininterrumpida• Número de personas formadas en normas de salud y seguridad
Actividades	Nivel de Capacidad
<ul style="list-style-type: none">• Examinar los requisitos de protección de las instalaciones de TI con respecto a las fluctuaciones y cortes eléctricos, junto con otros requisitos de planificación de continuidad del negocio.• Procurar un equipo de suministro ininterrumpido adecuado (ej. baterías, generadores) para respaldar la planificación de continuación del negocio.	2
<ul style="list-style-type: none">• Probar regularmente los mecanismos de suministro eléctrico ininterrumpidos.• Asegurar que la electricidad pueda cambiar a otra fuente de alimentación sin ningún efecto significativo en las operaciones del negocio.	
<ul style="list-style-type: none">• Asegurar que las instalaciones que acogen los sistemas de I&T cuenten con más de una fuente para las utilidades de servicios dependientes (ej. electricidad, telecomunicaciones, agua, gas).• Separar la entrada física de cada utilidad de servicio.	
<ul style="list-style-type: none">• Confirmar que el cableado exterior de la instalación de TI se sitúe bajo tierra o tenga una protección alternativa adecuada.• Determinar que el cableado de la instalación de TI se encuentre en conductos seguros, y el acceso a armarios de cableado esté restringido a personal autorizado.• Proteger el cableado adecuadamente frente al daño causado por el fuego, el humo, el agua, la intercepción y la interferencia.	
<ul style="list-style-type: none">• Asegurar que el cableado y los parches de cableado físico (datos y teléfono) estén estructurados y organizados.• Las estructuras de cableado y conducción deberían estar documentadas (ej. diagramas de cableado y planos de construcción).	
<ul style="list-style-type: none">• Educación al personal de forma regular sobre la legislación, las regulaciones y directrices en salud y seguridad relevantes.• Educación al personal sobre simulacros de incendio y rescate para garantizar el conocimiento y las acciones tomadas en caso de fuego o incidentes similares.	



Gestionar las Operaciones

Componente: Procesos

Práctica de Gestión		Métricas Modelo	
DSS01.05 Gestionar las instalaciones. Gestionar las instalaciones, incluidos los equipos de suministro eléctrico y comunicaciones, alineados con las leyes y reglamentos existentes, los requisitos técnicos y del negocio, las especificaciones del proveedor, y las directrices de salud y seguridad.		<ul style="list-style-type: none">• Tiempo transcurrido desde la última prueba del suministro de energía ininterrumpida• Número de personas formadas en normas de salud y seguridad	
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">• Asegurar que las instalaciones y el equipo de TI se mantengan conforme a los intervalos y especificaciones de servicio recomendados por el proveedor.• Asegurar que el mantenimiento se realice solo por personal autorizado.			3
<ul style="list-style-type: none">• Analizar los sistemas de alojamiento de alta disponibilidad de las instalaciones para comprobar redundancia y requisitos de cableado a prueba de fallos (externo e interno).			
<ul style="list-style-type: none">• Asegurar que las instalaciones de TI cumplen con la legislación, regulaciones y, directrices de salud y seguridad y, las especificaciones de proveedores relevantes.			
<ul style="list-style-type: none">• Registrar, monitorizar, gestionar y resolver incidentes en las instalaciones en línea con el proceso de gestión de incidentes de I&T.• Poner a disposición informes sobre incidentes en las instalaciones que la legislación y las regulaciones obligan a hacer públicos.			4
<ul style="list-style-type: none">• Analizar las alteraciones físicas de las instalaciones de TI para reevaluar el riesgo medioambiental (ej. daño por fuego o agua).• Informar los resultados de este análisis a la dirección de instalaciones y continuidad del negocio.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin documentación relacionada para esta práctica de gestión			



Gestionar las Operaciones

Componentes: Estructuras Organizativas

	D i r e c t o r d e o p e r a c i o n e s	D i r e c t o r d e T I	D i r e c t o r d e t e c n o l o g í a	J e f e d e o p e r a c i o n e s d e T I	G e s t o r d e s e g u r i d a d d e l a i n f o r m a c i ó n	D i r e c t o r d e p r i v a c i d a d
Práctica clave de gestión						
DSS01.01 Ejecutar procedimientos operativos.	R	A	R	R		
DSS01.02 Gestionar servicios tercerizados de I&T.		A	R	R	R	R
DSS01.03 Monitorizar la infraestructura de I&T		R	A	R	R	
DSS01.04 Gestionar el medioambiente.		R	A	R	R	
DSS01.05 Gestionar las instalaciones		R	A	R	R	



Gestionar las Operaciones

Componentes: Flujos y elementos de información

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS01.01 Ejecutar procedimientos operativos.	BAI05.05	Plan de operación y uso	Registro de copias de seguridad	Interna
			Calendario operativo	Interna
DSS01.02 Gestionar servicios tercerizados de I&T.	APO09.03	• SLA • OLA	Planes independientes de aseguramiento	MEA04.02
	BAI05.05	Plan de operación y uso		
DSS01.03 Monitorizar la infraestructura de I&T.	BAI03.11	Definiciones de servicios	Reglas de monitorización de activos y estados de eventos	DSS02.01; DSS02.02
			Tickets de incidentes	DSS02.02
			Logs de eventos	Interna
DSS01.04 Gestionar el medioambiente.			Políticas medioambientales.	APO01.09
			Informes de políticas de seguros	MEA03.03
DSS01.05 Gestionar las instalaciones.			Concienciación de salud y seguridad	Interna
			Informes de evaluación de instalaciones	MEA01.03
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)			Referencia específica	
National Institute of Standards and Technology Special Publication 800–37, Revisión 2, septiembre de 2017			3.2 Categorization (Task 5, 6): Inputs and Outputs	



Gestionar las Operaciones

Componentes: Personas, habilidades y competencias

Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Administración de bases de datos	Skills Framework for the Information Age V6, 2015	DBAD
Gestión de instalaciones	Skills Framework for the Information Age V6, 2015	DCMA
Infraestructura de TI	Skills Framework for the Information Age V6, 2015	ITOP
Métodos y herramientas	Skills Framework for the Information Age V6, 2015	METL
Prestación de servicios	e-Competence Framework (e-CF) – A common European Framework for ICT Professionals in all industry sectors – Part 1: Framework, 2016	C. Run – C.3. Service Delivery
Gestión de almacenamiento	Skills Framework for the Information Age V6, 2015	STMG



Gestionar las Operaciones

Componentes: Políticas y procedimientos

Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de gestión de servicios	<ul style="list-style-type: none">• Proporciona dirección y directrices para garantizar la gestión e implementación efectiva de todos los servicios de I&T para satisfacer los requisitos del negocio y del cliente, dentro de un marco de mediciones del rendimiento.• Cubre la gestión de riesgos relacionados con los servicios de I&T.• (El marco ITIL V3 ofrece directrices detalladas para la gestión de servicios y la optimización del riesgo relacionado con los servicios.).	(1) ISO/IEC 20000–1:2011(E); (2) ITIL V3, 2011	(1) 4.1.2 Service management policy (2) Service Strategy, 3. Service strategy principles



Gestionar las Operaciones

Componentes: Cultura, ética y comportamiento

Elementos culturales clave	Documentación relacionada	Referencia específica
<ul style="list-style-type: none">• Crear una cultura habitual de excelencia en toda la organización.• Animar a los empleados a sobresalir.• Crear un entorno en el que los procedimientos operativos ofrezcan (más que) los servicios necesarios mientras que permitan a los empleados cuestionar el status quo y probar nuevas ideas.• Gestionar la excelencia operativa a través del compromiso de los empleados y la mejora continua.• Aplicar el enfoque centrado en el cliente (tanto para clientes internos y externos).		



Gestionar las Operaciones

Componentes: Servicios, infraestructura y aplicaciones

- Servicios de alojamiento en la nube.
- Herramientas de monitorización de infraestructura.
- Herramientas de supervisión del nivel de servicio.



Gestionar las Operaciones

Resumen de Procesos de Gestionar las Operaciones

- DSS01.01 Ejecutar procedimientos operativos.
- DSS01.02 Gestionar servicios tercerizados de I&T.
- DSS01.03 Monitorizar la infraestructura de I&T.
- DSS01.04 Gestionar el medioambiente.
- DSS01.05 Gestionar las instalaciones.





Gestionar las Operaciones

Algunos Conceptos Clave

- **Observability**
- La observabilidad TI se refiere a la capacidad de comprender, analizar y depurar sistemas complejos, como aplicaciones informáticas o infraestructuras de TI, a través de la recopilación y el análisis de datos operativos.
- Se logra mediante el uso de herramientas y prácticas que permiten a los equipos de desarrollo y operaciones monitorear y analizar el comportamiento de los sistemas en tiempo real.
- Los principios básicos de la observabilidad TI incluyen la instrumentación adecuada de los sistemas para recopilar datos relevantes, la capacidad de correlacionar estos datos para identificar patrones y problemas, y la presentación de la información de manera comprensible para los equipos técnicos.
- En resumen, ayuda a los equipos a comprender mejor el rendimiento y el comportamiento de los sistemas, lo que les permite identificar y solucionar problemas de manera más eficiente.





Gestionar las Operaciones

Algunos Conceptos Clave

- **XAAS – Everything as a Service**
- “Cualquier cosa como servicio” se refiere al modelo de entrega de servicios a través de Internet.
- En este modelo, los servicios se ofrecen de forma remota a través de la nube, lo que permite a las organizaciones acceder a ellos según sea necesario sin tener que mantener la infraestructura localmente.





Gestionar las Operaciones

Algunos Conceptos Clave

- **SAAS – Software as a Service**

- El software como servicio se refiere a un modelo de distribución de software donde el software se aloja en la nube y se ofrece a los usuarios a través de Internet.
- En lugar de comprar y descargar software en sus dispositivos, los usuarios pueden acceder al software a través de un navegador web. En el modelo SaaS, los usuarios generalmente pagan una tarifa periódica, como mensual o anual, para acceder al software.
- Esta tarifa suele incluir el mantenimiento, las actualizaciones y el soporte técnico, lo que hace que sea más fácil y rentable para las organizaciones utilizar el software sin tener que preocuparse por la infraestructura subyacente.
- Algunos ejemplos comunes de software ofrecido como servicio incluyen aplicaciones de productividad empresarial, como suites de oficina y herramientas de colaboración, servicios de gestión empresarial, como CRM (Customer Relationship Management, o Gestión de Relaciones con los Clientes), y aplicaciones de marketing digital, entre otros.
- En resumen, SaaS es un modelo de distribución de software que ofrece una forma flexible y rentable para que las organizaciones accedan y utilicen software sin tener que preocuparse por la gestión de la infraestructura subyacente.





Gestionar las Operaciones

Algunos Conceptos Clave

- **STAAS – Storage as a Service**
- El almacenamiento como servicio se refiere a la prestación de servicios de almacenamiento de datos a través de la nube.
- En este modelo, las organizaciones pueden almacenar sus datos en servidores remotos mantenidos por un proveedor de servicios en la nube, en lugar de mantener su propio hardware de almacenamiento.
- STAAS ofrece una serie de beneficios, como la escalabilidad, ya que las organizaciones pueden aumentar o disminuir su capacidad de almacenamiento según sea necesario sin tener que invertir en hardware adicional.
- También puede ser más rentable, ya que las organizaciones solo pagan por el almacenamiento que utilizan. Además, STAAS puede incluir características como copias de seguridad automatizadas, recuperación ante desastres y almacenamiento de datos redundante para garantizar la seguridad y la disponibilidad de los datos.
- En resumen, STAAS es un modelo de servicio que permite a las organizaciones almacenar sus datos de forma remota a través de la nube, ofreciendo flexibilidad, escalabilidad y seguridad para sus necesidades de almacenamiento de datos.





Gestionar las Operaciones

Algunos Conceptos Clave

- **IAAS – Infrastructure as a Service**
- La infraestructura como servicio se refiere a un modelo de distribución de computación en la nube en el que un proveedor de servicios de la nube ofrece a los usuarios infraestructura de TI, como servidores virtuales, redes, almacenamiento y sistemas operativos, a través de Internet.
- En el modelo IaaS, los usuarios pueden acceder a recursos de infraestructura de TI según sea necesario, en lugar de tener que comprar y mantener su propia infraestructura física.
- Esto les permite escalar sus recursos de forma rápida y eficiente, pagando solo por los recursos que realmente utilizan.
- Algunos ejemplos de servicios IaaS incluyen máquinas virtuales, almacenamiento en la nube, redes definidas por software (SDN) y servicios de equilibrio de carga.
- En resumen, IaaS es un modelo de computación en la nube que ofrece a las organizaciones acceso a infraestructura de TI escalable y bajo demanda a través de Internet, lo que les permite reducir costos y mejorar la flexibilidad de sus operaciones de TI.





Gestionar las Operaciones

Algunos Conceptos Clave

- **PAAS – Platform as a Service**
- La plataforma como servicio se refiere a un modelo de computación en la nube en el que un proveedor de servicios de la nube ofrece a los usuarios una plataforma de desarrollo y despliegue de aplicaciones a través de Internet.
- En el modelo PaaS, los usuarios pueden desarrollar, ejecutar y gestionar aplicaciones sin tener que preocuparse por la infraestructura subyacente, como servidores, redes y sistemas operativos.
- La plataforma PaaS proporciona un entorno de desarrollo completo que incluye herramientas de desarrollo, bases de datos, middleware y servicios de implementación y escalabilidad.
- Algunos ejemplos de servicios PaaS incluyen Google App Engine, Microsoft Azure App Service y Heroku.
- En resumen, PaaS es un modelo de computación en la nube que ofrece a los desarrolladores una plataforma completa para desarrollar, ejecutar y gestionar aplicaciones sin tener que preocuparse por la infraestructura subyacente, lo que les permite centrarse en la creación de aplicaciones sin tener que preocuparse por la gestión de la infraestructura.





Universidad de Santiago de Chile
Facultad de Ingeniería
Departamento de Informática

Gestión y Gobernanza TI

Gestionar las Peticiones y los
Incidentes de Servicio



Gestionar las Peticiones y los Incidentes de Servicio

Introducción

- DSS02 – Gestionar las peticiones y los incidentes de servicio.
- Pertenece al Dominio de Gestión Entregar, Dar Servicio y Soporte (DSS – Deliver, Service and Support).





Gestionar las Peticiones y los Incidentes de Servicio

Introducción



Entregar, Dar Servicio y Soporte (DSS – Deliver, Service and Support)



Gestionar las Peticiones y los Incidentes de Servicio

Descripción

- Proporcionar una respuesta oportuna y efectiva a las solicitudes de los usuarios y la resolución de todos los tipos de incidentes.
- Restaurar el servicio normal, registrar y completar las solicitudes de usuario; y registrar, investigar, diagnosticar, escalar y resolver los incidentes.





Gestionar las Peticiones y los Incidentes de Servicio

Propósito

- Lograr una mayor productividad y minimizar las interrupciones mediante la resolución rápida de consultas e incidencias de los usuarios.
- Evaluar el impacto de los cambios y hacer frente a los incidentes del servicio.
- Resolver las solicitudes de los usuarios y restaurar el servicio como respuesta ante incidentes.





Gestionar las Peticiones y los Incidentes de Servicio

Componentes


- Procesos (7):
 - DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio.
 - DSS02.02 Registrar, clasificar y priorizar las peticiones e incidentes.
 - DSS02.03 Verificar, aprobar y resolver peticiones de servicio.
 - DSS02.04 Investigar, diagnosticar y asignar incidentes.
 - DSS02.05 Resolver y recuperarse de los incidentes.
 - DSS02.06 Cerrar las peticiones de servicio y los incidentes.
 - DSS02.07 Hacer seguimiento al estado y producir informes.
- Estructuras organizativas.
- Flujos y elementos de información.
- Personas, habilidades y competencias (5).
- Políticas y procedimientos (1).
- Cultura, ética y comportamiento (1).
- Servicios, infraestructura y aplicaciones (1).





Gestionar las Peticiones y los Incidentes de Servicio

El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:

Metas Empresariales			Metas de Alineamiento	
<ul style="list-style-type: none">EG01 – Portafolio de productos y servicios competitivosEG08 – Optimización de la funcionalidad de procesos internos del negocio			<ul style="list-style-type: none">AG05 – Prestación de servicios de I&T en línea con los requisitos del negocio	
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento	
EG01	<ul style="list-style-type: none">Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercadoPorcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del clientePorcentaje de productos y servicios que proporcionan una ventaja competitivaPlazo de comercialización para nuevos productos y servicios		AG05	<ul style="list-style-type: none">Porcentaje de partes interesadas del negocio satisfechas con que la prestación de servicios de I&T cumpla con los niveles de servicio acordadosNúmero de interrupciones del negocio debido a incidentes de servicios de I&TPorcentaje de usuarios satisfechos con la calidad de la prestación de servicios de I&T
EG08	<ul style="list-style-type: none">Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarialNiveles de satisfacción de los clientes con las capacidades de prestación de serviciosNiveles de satisfacción de los proveedores con las capacidades de la cadena de suministro			



Gestionar las Peticiones y los Incidentes de Servicio

Componente: Procesos

Práctica de Gestión		Métricas Modelo	
DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio. Definir esquemas de clasificación y modelos de incidentes y de peticiones de servicio.		<ul style="list-style-type: none">Número total de solicitudes e incidentes de servicio por nivel de prioridadNúmero total de incidentes escalados	
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">Definir esquemas de priorización y clasificación de solicitudes de servicios e incidentes, y los criterios para el registro de problemas.Usar esta información para garantizar estrategias constantes a fin de gestionar e informar a los usuarios sobre los problemas y llevar a cabo análisis de tendencias.			2
<ul style="list-style-type: none">Definir modelos de incidentes sobre errores conocidos para permitir una resolución eficiente y eficaz.			
<ul style="list-style-type: none">Definir modelos de solicitud de servicios conforme al tipo de solicitud de servicios para permitir la autoayuda y un servicio eficiente para solicitudes estándar.			
<ul style="list-style-type: none">Definir las reglas y procedimientos de escalamiento de incidentes, sobre todo para incidentes importantes e incidentes de seguridad.			
<ul style="list-style-type: none">Definir las fuentes de conocimiento sobre incidentes y solicitudes y describir cómo usarlas.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
CMMI Cybermaturity Platform, 2018		IA.IP Implement Incident Investigation Processes	
HITRUST CSF versión 9, septiembre de 2017		11.01 Reporting Information Security Incidents and Weaknesses	
ISF, The Standard of Good Practice for Information Security 2016		TM2 Security Incident Management	
ISO/IEC 20000–1:2011(E)		8.1 Incident and service request management	
ISO/IEC 27002:2013/Cor.2:2015(E)		16. Information security incident management	



Gestionar las Peticiones y los Incidentes de Servicio

Componente: Procesos

Práctica de Gestión		Métricas Modelo	
DSS02.02 Registrar, clasificar y priorizar las peticiones e incidentes. Identificar, registrar y clasificar las peticiones de servicio y los incidentes, y asignarles una prioridad de acuerdo con la criticidad para el negocio y los acuerdos de servicio.		<ul style="list-style-type: none">Número de tipos y categorías definidos para registrar solicitudes e incidentes de servicioNúmero de solicitudes e incidentes de servicio no clasificados	
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">Registrar todas las solicitudes e incidentes de servicio, mediante el registro de toda la información relevante, para que pueda gestionarse de forma eficaz y pueda mantenerse un registro histórico completo.			2
<ul style="list-style-type: none">Permitir el análisis de tendencias, clasificar las solicitudes e incidentes de servicio, con identificación del tipo y categoría.			
<ul style="list-style-type: none">Priorizar solicitudes e incidentes de servicio basados en la definición del servicio de SLA según el impacto y la urgencia para el negocio.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin documentación relacionada para esta práctica de gestión			



Gestionar las Peticiones y los Incidentes de Servicio

Componente: Procesos

Práctica de Gestión		Métricas Modelo	
DSS02.03 Verificar, aprobar y resolver peticiones de servicio. <ul style="list-style-type: none">• Seleccionar los procedimientos apropiados para peticiones y verificar que las solicitudes de servicio cumplan con los criterios de solicitud definidos.• Obtener aprobación, si se requiere, y satisfacer las solicitudes.		<ul style="list-style-type: none">• Tiempo promedio transcurrido para la gestión de cada tipo de solicitud de servicio• Porcentaje de solicitudes de servicio que cumplen con los criterios de solicitud definidos	
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">• Comprobar el derecho a las solicitudes de servicio, utilizando un flujo de proceso predefinido y cambios estándar, cuando sea posible.			2
<ul style="list-style-type: none">• Obtener la aprobación y confirmación financiera y funcional, si fuera necesario, o las aprobaciones predefinidas para los cambios estándar acordados.			
<ul style="list-style-type: none">• Cumplir con las solicitudes realizando el proceso de solicitud seleccionado.• Cuando sea posible, usar menús automáticos de autoayuda y modelos de solicitud predefinidas para elementos solicitados con frecuencia.			3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
ITIL V3, 2011		Service Operation, 4.3 Request Fulfilment	



Gestionar las Peticiones y los Incidentes de Servicio

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS02.04 Investigar, diagnosticar y asignar incidentes. Identificar y registrar los síntomas de los incidentes, determinar las causas posibles y asignarlos para su resolución.	<ul style="list-style-type: none">• Número de síntomas de incidentes identificados y registrados• Número de causas de síntomas correctamente determinadas• Número de problemas duplicados en el log de referencia	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">• Identificar y describir síntomas relevantes para establecer las causas más probables de los incidentes.• Referenciar los recursos de conocimientos disponibles (incluidos errores y problemas conocido) para identificar posibles resoluciones de incidentes (soluciones temporales y/o permanentes).		2
<ul style="list-style-type: none">• Si un problema relacionado o error conocido no existe todavía y si el incidente satisface los criterios acordados para el registro de problemas, registrarlo como un problema nuevo.		
<ul style="list-style-type: none">• Asignar incidentes a funciones de especialista si se necesita una mayor habilidad.• Contar con el nivel directivo adecuado, donde y si se necesita.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
Sin documentación relacionada para esta práctica de gestión		



Gestionar las Peticiones y los Incidentes de Servicio

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS02.05 Resolver y recuperarse de los incidentes. <ul style="list-style-type: none">Documentar, aplicar y probar las soluciones definitivas o temporales (workarounds) identificados.Realizar acciones de recuperación para restaurar el servicio relacionado con I&T.	<ul style="list-style-type: none">Porcentaje de incidentes resueltos dentro de los SLA acordadosPorcentaje de satisfacción de las partes interesadas con la solución y recuperación del incidente	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">Seleccionar y aplicar las resoluciones de incidentes más adecuadas (solución workaround y/o solución permanente).		2
<ul style="list-style-type: none">Registrar, si se usaron, workarounds para la resolución de incidentes.		
<ul style="list-style-type: none">Aplicar medidas correctivas, si se requieren.		
<ul style="list-style-type: none">Documentar la resolución de incidentes y evaluar si la resolución puede usarse como una fuente de conocimiento futura.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ITIL V3, 2011		Service Operation, 4.2 Incident Management
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, abril de 2018		RC.RP Recovery Planning
National Institute of Standards and Technology Special Publication 800–53, Revisión 5 (Borrador), agosto de 2017		3.9 Incident response (IR–4, IR–5, IR–6)
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, Agosto de 201		CSC 19: Incident Response and Management



Gestionar las Peticiones y los Incidentes de Servicio

Componente: Procesos

Práctica de Gestión		Métricas Modelo	
DSS02.06 Cerrar las peticiones de servicio y los incidentes. Verificar la solución satisfactoria del incidente y/o el cumplimiento de la petición y su cierre.		<ul style="list-style-type: none">Nivel de satisfacción del usuario con el cumplimiento de la petición de servicioPorcentaje de incidentes resueltos dentro del periodo de tiempo acordado/ aceptado	
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">Comprobar con los usuarios afectados que la solicitud de servicio se ha cumplido de forma satisfactoria o el incidente se ha resuelto de forma satisfactoria dentro de un plazo de tiempo acordado/aceptable.			2
<ul style="list-style-type: none">Cerrar las peticiones e incidentes de servicio.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin documentación relacionada para esta práctica de gestión			



Gestionar las Peticiones y los Incidentes de Servicio

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS02.07 Hacer seguimiento al estado y producir informes. <ul style="list-style-type: none">Hacer seguimiento, analizar e informar regularmente sobre los incidentes y el cumplimiento de las solicitudes.Examinar tendencias para proporcionar información para la mejora continua.	<ul style="list-style-type: none">Tiempo promedio entre incidentes para el servicio habilitado por I&TNúmero y porcentaje de incidentes que causan interrupciones en procesos críticos del negocio	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">Supervisar y hacer seguimiento al escalamientos y resoluciones de incidentes y solicitar procedimientos de manejo para progresar hacia la resolución o finalización de los mismos.		2
<ul style="list-style-type: none">Identificar las partes interesadas en la información y sus necesidades de datos o informes.Identificar frecuencia y medio de elaboración de los reportes.		3
<ul style="list-style-type: none">Producir y distribuir informes en el plazo debido o proporcionar un acceso controlado a los datos en línea.		4
<ul style="list-style-type: none">Analizar incidentes y solicitudes de servicio por categoría y tipo.Establecer tendencias e identificar patrones de problemas recurrentes, violaciones o ineficiencias del SLA.		
<ul style="list-style-type: none">Usar la información como un insumo a la planificación de la mejora continua.		5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		MI.IM Ensure Incident Mitigation; IR.IR Incident Reporting
National Institute of Standards and Technology Special Publication 800–53, Revisión 5 (Borrador), agosto de 2017		3.9 Incident response (IR–7, IR–8)



Gestionar las Peticiones y los Incidentes de Servicio

Componentes: Estructuras Organizativas

	D i r e c t o r d e t e c n o l o g í a	Du e ñ o s d e l p r o c e s o d e n e g o c i o	J e f e d e d e s a r r o l l o	J e f e d e o p e r a c i o n e s d e T I	G e s t o r d e s e r v i c i o	G e s t o r d e s e g u r i d a d d e l a i n f o r m a c i ó n
Práctica clave de gestión						
DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio.	A		R	R	R	
DSS02.02 Registrar, clasificar y priorizar las peticiones e incidentes.	A			R	R	
DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	A	R	R	R	R	
DSS02.04 Investigar, diagnosticar y asignar incidentes.	A	R		R	R	
DSS02.05 Resolver y recuperarse de los incidentes.	A		R	R	R	R



Gestionar las Peticiones y los Incidentes de Servicio

Componentes: Flujos y elementos de información

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio.	APO09.03	SLA	Criterios para el registro de problemas	DSS03.01
	BAI10.02	Repositorio de configuraciones	Reglas para escalamiento de incidentes	Interna
	BAI10.03	Repositorio actualizado con elementos de configuración	Esquema y modelos de clasificación de peticiones de servicio e incidentes	Interna
	BAI10.04	Informes de estado de la configuración		
	DSS01.03	Reglas de monitorización de activos y estado de eventos		
	DSS03.01	Esquema de clasificación de problemas		
	DSS04.03	Acciones y comunicaciones para responder a incidentes		



Gestionar las Peticiones y los Incidentes de Servicio

Componentes: Flujos y elementos de información

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS02.02 Registrar, clasificar y priorizar las peticiones e incidentes.	APO09.03	SLA	Peticiones de servicio e incidentes clasificadas y priorizadas	APO08.03; APO09.04; APO13.03; DSS03.05
	BAI04.05	Procedimiento de escalamiento de emergencia	Registro de solicitudes de servicio e incidentes	Interna; MEA04.07
	DSS01.03	<ul style="list-style-type: none">Reglas de monitorización de activos y estado de eventosTickets de incidentes		
	DSS05.07	Tickets de incidentes relacionados con la seguridad		
DSS02.03: Verificar, aprobar y resolver peticiones de servicio.	APO12.06	Causas raíz relacionadas con el riesgo	Peticiones de servicio aprobadas	BAI06.01
			Peticiones de servicio completadas	Interna
DSS02.04 Investigar, diagnosticar y asignar incidentes.	BAI07.07	Plan de soporte suplementario	Log de problemas	DSS03.01
			Síntomas de incidente	Interna



Gestionar las Peticiones y los Incidentes de Servicio

Componentes: Flujos y elementos de información

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS02.05 Resolver y recuperarse de los incidentes.	APO12.06	Plan de respuesta a incidentes relacionados con riesgos	Resoluciones de incidentes	DSS03.03; DSS03.04; DSS03.05; MEA04.07
	DSS03.03	Registros de errores conocidos		
	DSS03.04	Comunicación de conocimientos aprendidos		
DSS02.06 Cerrar las peticiones de servicio y los incidentes.	DSS03.04	Registros de problemas cerrados	Confirmación del usuario del cumplimiento o resolución satisfactoria	APO08.03
			Cierre de peticiones de servicio e incidentes	APO08.03; APO09.04; DSS03.04



Gestionar las Peticiones y los Incidentes de Servicio

Componentes: Flujos y elementos de información

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS02.07 Hacer seguimiento al estado y producir informes.	APO09.03	OLAs	Estado de incidentes e informe de tendencias	APO08.03; APO09.04; APO11.04; APO12.01; MEA01.03
	DSS03.01	Informe de estado del problema	Estado de cumplimiento de peticiones e informe de tendencias	APO08.03; APO09.04; APO11.04; DSS03.02; MEA01.03
	DSS03.02	Informes de resolución de problemas		
	DSS03.05	Informes de monitorización de resolución de problemas		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica		
Sin documentación relacionada para este componente.				



Gestionar las Peticiones y los Incidentes de Servicio

Componentes: Personas, habilidades y competencias

Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Soporte de aplicaciones	Skills Framework for the Information Age V6, 2015	ASUP
Servicio de atención al cliente	Skills Framework for the Information Age V6, 2015	CSMG
Gestión de incidentes	Skills Framework for the Information Age V6, 2015	USUP
Soporte de redes	Skills Framework for the Information Age V6, 2015	NTAS
Soporte de usuarios	Skills Framework for the Information Age V6, 2015	C. Run – C.1. User Support



Gestionar las Peticiones y los Incidentes de Servicio

Componentes: Políticas y procedimientos

Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de solicitud de servicio	<ul style="list-style-type: none">Establece los fundamentos y proporciona directrices para las peticiones de servicio e incidentes y su documentación.	ITIL V3, 2011	Service Operation, 3. Service operation principles



Gestionar las Peticiones y los Incidentes de Servicio

Componentes: Cultura, ética y comportamiento

Elementos culturales clave	Documentación relacionada	Referencia específica
<ul style="list-style-type: none">• Permitir a los empleados identificar incidentes de forma correcta y en el plazo debido e implementar las rutas de escalamiento adecuadas.• Fomentar la prevención.• Responder y resolver los incidentes de forma inmediata.• Evitar una cultura de héroes.		



Gestionar las Peticiones y los Incidentes de Servicio

Componentes: Servicios, infraestructura y aplicaciones

- Sistema y herramientas de seguimiento de incidentes.



Gestionar las Peticiones y los Incidentes de Servicio

Resumen de Procesos de Gestionar las Peticiones y los Incidentes de Servicio

- DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio.
- DSS02.02 Registrar, clasificar y priorizar las peticiones e incidentes.
- DSS02.03 Verificar, aprobar y resolver peticiones de servicio.
- DSS02.04 Investigar, diagnosticar y asignar incidentes.
- DSS02.05 Resolver y recuperarse de los incidentes.
- DSS02.06 Cerrar las peticiones de servicio y los incidentes.
- DSS02.07 Hacer seguimiento al estado y producir informes.





Gestionar las Peticiones y los Incidentes de Servicio

Algunos Conceptos Clave

- **Service Desk**
- La mesa de servicios es una función dentro de una organización que se encarga de brindar soporte y asistencia a los usuarios o clientes en relación con los servicios de TI.
- Su objetivo principal es resolver problemas y solicitudes de servicio de manera eficiente y oportuna, garantizando la satisfacción del usuario final.
- El Service Desk suele ser el primer punto de contacto para los usuarios que necesitan ayuda con problemas técnicos, consultas o solicitudes de servicios.
- Puede proporcionar asistencia a través de diferentes canales, como el teléfono, el correo electrónico, el chat en línea o un sistema de tickets.
- Además de resolver problemas, el Service Desk también se encarga de gestionar y coordinar las solicitudes de servicio más complejas que requieren la intervención de otros equipos de TI.
- En resumen, el Service Desk es fundamental para garantizar que los servicios de TI se entreguen de manera efectiva, ayudando a minimizar el tiempo de inactividad y a mantener la productividad de los usuarios finales.





Gestionar las Peticiones y los Incidentes de Servicio

Algunos Conceptos Clave

- **KEBD – Knowledge and Error Database**
- La base de datos de errores conocidos contiene información detallada sobre problemas anteriores, soluciones y errores conocidos en un entorno de TI.
- Esta base de datos se utiliza para ayudar en la resolución rápida de problemas recurrentes y para mejorar la eficiencia del soporte técnico al proporcionar un repositorio centralizado de conocimiento sobre errores y soluciones.
- El KEDB es una herramienta importante en la gestión de incidentes y problemas, ya que permite a los equipos de soporte resolver problemas de manera más eficiente al aprovechar la información y las soluciones que se han recopilado y documentado previamente.





Gestionar las Peticiones y los Incidentes de Servicio

Algunos Conceptos Clave

- **CMS – Configuration Management System**
- El sistema de gestión de la configuración se utiliza en la gestión de la configuración de software y sistemas de tecnología de la información (TI).
- Su objetivo principal es controlar y documentar de manera sistemática todos los elementos que componen un sistema, desde el software y hardware hasta la documentación y los datos.
- En un entorno de TI, un CMS es fundamental para asegurar la integridad, consistencia y trazabilidad de la configuración de los sistemas y componentes o largo de su ciclo de vida.
- Permite gestionar cambios, controlar versiones, identificar y resolver discrepancias, y proporcionar un registro histórico detallado de la configuración de los sistemas.
- Un CMS puede incluir herramientas de control de versiones, bases de datos de configuración, sistemas de seguimiento de cambios, documentación de configuración, entre otros componentes que ayudan a garantizar la estabilidad y la eficiencia en la gestión de la configuración de sistemas de TI.





Universidad de Santiago de Chile
Facultad de Ingeniería
Departamento de Informática

Gestión y Gobernanza TI

Gestionar los Problemas



Gestionar los Problemas

Introducción

- DSS03 – Gestionar los Problemas.
- Pertenece al Dominio de Gestión Entregar, Dar Servicio y Soporte (DSS – Deliver, Service and Support).





Gestionar los Problemas

Introducción

EDM01—Garantizar el establecimiento y el mantenimiento del marco de gobierno

EDM02—Asegurar la realización de beneficios

EDM03—Asegurar la optimización del riesgo

EDM04—Asegurar la optimización de los recursos

EDM05—Asegurar la transparencia de las partes interesadas

APO01—Gestionar el marco de gestión de TI

APO02—Gestionar la estrategia

APO03—Gestionar la arquitectura de la empresa

APO04—Gestionar la innovación

APO05—Gestionar el portafolio

APO06—Gestionar el presupuesto y los costes

APO07—Gestionar los recursos humanos

APO08—Gestionar las relaciones

APO09—Gestionar los acuerdos de servicio

APO10—Gestionar los proveedores

APO11—Gestionar la calidad

APO12—Gestionar el riesgo

APO13—Gestionar la seguridad

APO14—Gestionar los datos

MEA01—Gestionar la monitorización del rendimiento y la conformidad

BAI01—Gestionar los programas

BAI02—Gestionar la definición de requisitos

BAI03—Gestionar la identificación y construcción de soluciones

BAI04—Gestionar la disponibilidad y capacidad

BAI05—Gestionar los cambios organizativos

BAI06—Gestionar los cambios de TI

BAI07—Gestionar la aceptación y la transición de los cambios de TI

MEA02—Gestionar el sistema de control interno

BAI08—Gestionar el conocimiento

BAI09—Gestionar los activos

BAI10—Gestionar la configuración

BAI11—Gestionar los proyectos

MEA03—Gestionar el cumplimiento de los requisitos externos

DSS01—Gestionar las operaciones

DSS02—Gestionar las solicitudes e incidentes de servicio

DSS03—Gestionar los problemas

DSS04—Gestionar la continuidad

DSS05—Gestionar los servicios de seguridad

DSS06—Gestionar los controles de procesos de negocio

MEA04—Gestionar el aseguramiento

Entregar, Dar Servicio y Soporte (DSS – Deliver, Service and Support)



Gestionar los Problemas

Descripción

- Identificar y clasificar los problemas y su causa raíz. Ofrecer una solución oportuna para evitar incidentes recurrentes.
- Ofrecer recomendaciones de mejoras.





Gestionar los Problemas

Propósito

- Aumentar la disponibilidad, mejorar los niveles de servicio, reducir los costes y atender mejor las necesidades del cliente y lograr su satisfacción mediante una reducción del número de problemas operativos, e identificar las causas raíz como parte de la resolución de problemas.





Gestionar los Problemas

Componentes


- Procesos (5):
 - DSS03.01 Identificar y clasificar los problemas.
 - DSS03.02 Investigar y diagnosticar problemas.
 - DSS03.03 Presentar los errores conocidos.
 - DSS03.04 Resolver y cerrar los problemas.
 - DSS03.05 Realizar una gestión proactiva de los problemas.
- Estructuras organizativas.
- Flujos y elementos de información.
- Personas, habilidades y competencias (4).
- Políticas y procedimientos (1).
- Cultura, ética y comportamiento (1).
- Servicios, infraestructura y aplicaciones (1).





Gestionar los Problemas

El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:

Metas Empresariales			Metas de Alineamiento	
<ul style="list-style-type: none">EG01 – Portafolio de productos y servicios competitivosEG08 – Optimización de la funcionalidad de procesos del negocio interno			<ul style="list-style-type: none">AG05 – Prestación de servicios de I&T conforme a los requisitos del negocio	
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento	
EG01	<ul style="list-style-type: none">Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercadoPorcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del clientePorcentaje de productos y servicios que proporcionan una ventaja competitivaPlazo de comercialización para nuevos productos y servicios		AG05	<ul style="list-style-type: none">Porcentaje de partes interesadas del negocio satisfechas con la prestación de servicios de I&T que cumple con los niveles de servicio acordadosNúmero de interrupciones del negocio debido a incidentes de servicios de I&TPorcentaje de usuarios satisfechos con la calidad de la prestación de servicios de I&T
EG08	<ul style="list-style-type: none">Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarialNiveles de satisfacción de los clientes con las capacidades de prestación de serviciosNiveles de satisfacción de los proveedores con las capacidades de la cadena de suministro			



Gestionar los Problemas

Componente: Procesos

Práctica de Gestión	Métricas Modelo
DSS03.01 Identificar y clasificar los problemas. <ul style="list-style-type: none">Definir e implementar criterios y procedimientos para identificar e informar sobre los problemas.Incluir la clasificación, categorización y priorización del problema.	<ul style="list-style-type: none">Porcentaje de incidentes mayores para los que se registraron problemasPorcentaje de incidentes resueltos conforme a los SLA acordadosPorcentaje de problemas identificados correctamente, incluida la clasificación, categorización y priorización de estos.
Actividades	Nivel de Capacidad
<ul style="list-style-type: none">Identificar problemas a través de la correlación de informes de incidentes, registros de errores y otros recursos que permitan la identificación de problemas.	2
<ul style="list-style-type: none">Gestionar todos los problemas formalmente con acceso a todos los datos relevantes.Incluir información del sistema de gestión de cambios de TI y de configuración/activo de TI y los detalles del incidente.	
<ul style="list-style-type: none">Definir grupos de soporte adecuados para ayudar en la identificación de problemas, análisis de la causa raíz y determinación de soluciones para respaldar la gestión de problemas.Determinar grupos de soporte conforme a las categorías predefinidas, como hardware, red, software, aplicaciones y software de soporte.	
<ul style="list-style-type: none">Definir niveles de prioridad a través de la consulta con el negocio para garantizar que la identificación del problema y el análisis de las causas raíz se gestionan en el plazo debido conforme a los SLA acordados.Basar los niveles de prioridad en el impacto y la urgencia del negocio.	
<ul style="list-style-type: none">Informar del estado de los problemas identificados a la mesa de servicio, para que los clientes y gestores de TI puedan mantenerse informados.	
<ul style="list-style-type: none">Mantener un único catálogo de gestión de problemas para registrar e informar sobre los problemas identificados.Usar el catálogo para establecer pistas de auditoría de los procesos de gestión de problemas incluido el estado de cada problema (es decir, abierto, reabierto, en curso o cerrado).	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
ISO/IEC 20000-1:2011(E)	8.2 Problem management



Gestionar los Problemas

Componente: Procesos

Práctica de Gestión		Métricas Modelo	
DSS03.02 Investigar y diagnosticar problemas. Investigar y diagnosticar problemas con la ayuda de expertos en la materia para evaluar y analizar su causa raíz.		<ul style="list-style-type: none">Número de problemas identificados clasificados como errores conocidosPorcentaje de problemas investigados y diagnosticados a lo largo de su ciclo de vida	
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">Identificar problemas que podrían ser errores conocidos mediante una comparación de los datos de incidentes con la base de datos de errores conocidos y sospechados (ej. aquellos comunicados por proveedores externos).Clasificar los problemas como errores conocidos.			3
<ul style="list-style-type: none">Asociar los elementos de configuración afectados con el error establecido/conocido.			
<ul style="list-style-type: none">Producir informes para comunicar el progreso a la hora de resolver problemas y gestionar el impacto continuo de los problemas no resueltos.Monitorizar el estado del proceso de manejo de problemas a lo largo de su ciclo de vida, incluyendo los insumos de la gestión de cambios y de la configuración de TI.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin documentación relacionada para esta práctica de gestión			



Gestionar los Problemas

Componente: Procesos

Práctica de Gestión		Métricas Modelo	
DSS03.03 Presentar los errores conocidos. Tan pronto como se identifiquen las causas raíz de los problemas, crear registros de los errores conocidos, documentar las soluciones temporales apropiadas e identificar las soluciones potenciales.		<ul style="list-style-type: none">Número de problemas con resolución satisfactoria que abordan las causas raízPorcentaje de satisfacción de las partes interesada con la identificación de las causas raíz, la creación de registros de errores conocidos y soluciones temporales adecuadas, y la identificación de soluciones potenciales	
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">Tan pronto como se identifiquen las causas raíz de los problemas, crear registros de los errores conocidos y desarrollar una solución temporal apropiada.			2
<ul style="list-style-type: none">Identificar, evaluar, priorizar y procesar (a través de la gestión de cambio de TI) soluciones a los errores conocidos, conforme al coste/beneficio del caso de negocio, el impacto y la urgencia.			3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin documentación relacionada para esta práctica de gestión			



Gestionar los Problemas

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS03.04 Resolver y cerrar los problemas. <ul style="list-style-type: none">Identificar e iniciar soluciones sostenibles dirigidas a la causa raíz del problema.Presentar solicitudes de cambio a través del proceso de gestión de cambio establecido, si es necesario, para resolver los errores.Asegurarse de que el personal afectado conoce las medidas adoptadas y los planes desarrollados para evitar que ocurran incidentes en el futuro.	<ul style="list-style-type: none">Reducir el número de incidentes recurrentes causados por problemas no resueltosPorcentaje de soluciones temporales definidas para los problemas abiertos	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">Cerrar los registros de problemas después de la confirmación sobre la eliminación exitosa del error conocido o después del acuerdo con el negocio sobre cómo gestionar el problema de forma alternativa.		2
<ul style="list-style-type: none">Informar a la mesa de servicio sobre el calendario de cierre de problemas (ej. el calendario para solucionar los errores conocidos, la posible solución temporal o el hecho de que el problema seguirá ahí hasta que se implemente el cambio) y las consecuencias de la estrategia llevada a cabo.Mantener a los usuarios y clientes afectados informados como corresponda.		
<ul style="list-style-type: none">A través del proceso de resolución, obtener informes regulares de gestión de cambios de TI relacionados con el progreso a la hora de resolver problemas y errores.		3
<ul style="list-style-type: none">Monitorizar el impacto continuo de los problemas y errores conocidos en los servicios.		4
<ul style="list-style-type: none">Revisar y confirmar la resolución satisfactoria de problemas mayores.		
<ul style="list-style-type: none">Asegurar que el conocimiento aprendido de la revisión se incorpore a la reunión de revisión de servicios con el cliente del negocio.		5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
Sin documentación relacionada para esta práctica de gestión		



Gestionar los Problemas

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS03.05 Realizar una gestión proactiva de los problemas. <ul style="list-style-type: none">Recopilar y analizar los datos operacionales (especialmente los registros del incidente y los cambios) para identificar las tendencias que están emergiendo que puedan indicar problemas.Guardar los registros de problemas para permitir su evaluación.	<ul style="list-style-type: none">Porcentaje de problemas registrados como parte de la actividad de gestión de problemas proactivaPorcentaje de partes interesadas satisfechas con la comunicación de información de problemas relacionados con cambios e incidentes de TI	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">Captar la información del problema relacionada con cambios e incidentes de I&T y comunicarla a las partes interesadas clave.Comunicar a través de informes y reuniones periódicas entre los dueños de los procesos de incidentes, problemas, cambios y gestión de la configuración para considerar los problemas recientes y las posibles acciones correctivas.		3
<ul style="list-style-type: none">Garantizar que los dueños y gestores de los procesos de gestión de incidentes, problemas, cambios y configuración se reúnan regularmente para comentar los problemas conocidos y los cambios planificados futuros.		
<ul style="list-style-type: none">Identificar e iniciar soluciones sostenibles (soluciones permanentes) que aborden la causa raíz.Presentar solicitudes de cambio a través de los procesos establecidos de gestión de cambios.		



Gestionar los Problemas

Componente: Procesos

Práctica de Gestión		Métricas Modelo	
DSS03.05 Realizar una gestión proactiva de los problemas. <ul style="list-style-type: none">Recopilar y analizar los datos operacionales (especialmente los registros del incidente y los cambios) para identificar las tendencias que están emergiendo que puedan indicar problemas.Guardar los registros de problemas para permitir su evaluación.		<ul style="list-style-type: none">Porcentaje de problemas registrados como parte de la actividad de gestión de problemas proactivaPorcentaje de partes interesadas satisfechas con la comunicación de información de problemas relacionados con cambios e incidentes de TI	
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">Permitir a la empresa supervisar los costes totales de los problemas, captar los esfuerzos de cambios derivados de las actividades del proceso de gestión de problemas (ej. soluciones a problemas y errores conocidos) e informar al respecto.			4
<ul style="list-style-type: none">Crear informes para supervisar la resolución de problemas en relación con los requisitos del negocio y los SLAs.Asegurar el escalamiento adecuado de los problemas, como comunicarlos al siguiente nivel directivo conforme a los criterios acordados, contactar con proveedores externos o consultar con el consejo asesor de cambios (CAB) para aumentar la prioridad de una solicitud de cambio urgente (RFC) para implementar una solución temporal.			
<ul style="list-style-type: none">Optimizar el uso de recursos y reducir el uso de soluciones temporales; hacer un seguimiento a las tendencias de los problemas.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
CMMI Cybermaturity Platform, 2018		MI.IC Ensure Incident Containment	
ITIL V3, 2011		Service Operation, 4.4 Problem Management	



Gestionar los Problemas

Componentes: Estructuras Organizativas

	C o m i t é E j e c u t i v o	D i r e c t o r d e T I	D i r e c t o r d e t e c n o l o g í a	J e f e d e d e s a r r o l l o	J e f e d e o p e r a c i o n e s d e T I	G e s t o r d e s e r v i c i o s	G e s t o r d e s e g u r i d a d e l a i n f o r m a c i ó n
Práctica clave de gestión							
DSS03.01 Identificar y clasificar los problemas.		R	A	R	R	R	
DSS03.02 Investigar y diagnosticar problemas.			A		R	R	R
DSS03.03 Presentar los errores conocidos.			A		R	R	R



Gestionar los Problemas

Componentes: Flujos y elementos de información

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS03.01 Identificar y clasificar los problemas.	APO12.06	Causas raíz relacionadas con el riesgo	Esquema de clasificación de problemas	DSS02.01
	DSS02.01	Criterios para el registro de problemas	Informes de estado del problema	DSS02.07
	DSS02.04	Log de problemas	Registro de problemas	Interna
DSS03.02 Investigar y diagnosticar problemas.	APO12.06	Causas raíz relacionadas con el riesgo	Informes de resolución de problemas	DSS02.07
			Causas raíz de problemas	Interna; DSS03.05
DSS03.03 Presentar los errores conocidos.	APO12.06	Causas raíz relacionadas con el riesgo	Soluciones propuestas a errores conocidos	BAI06.01
	DSS02.05	Resoluciones de incidentes	Registros de errores conocidos	DSS02.05
DSS03.04 Resolver y cerrar los problemas.	DSS02.05	Resoluciones de incidentes	Comunicación de conocimientos aprendidos	APO08.04; DSS02.05
	DSS02.06	Cierre de peticiones de servicio e incidentes	Registros de problemas cerrados	DSS02.06



Gestionar los Problemas

Componentes: Flujos y elementos de información

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS03.05 Realizar una gestión proactiva de los problemas.	APO12.06	Causas raíz relacionadas con el riesgo	Soluciones sostenibles identificadas	BAI06.01
	DSS02.02	• Peticiones de servicio e incidentes clasificadas y priorizadas • Resoluciones de Incidentes	Informes de supervisión de resolución de problemas	DSS02.07, MEA04.07
	DSS03.04	Causas raíz de los problemas		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)			Referencia específica	
Sin documentación relacionada para este componente.				



Gestionar los Problemas

Componentes: Personas, habilidades y competencias

Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Soporte de aplicaciones	Skills Framework for the Information Age V6, 2015	ASUP
Soporte de redes	Skills Framework for the Information Age V6, 2015	NTAS
Gestión de problemas	e-Competence Framework (e-CF) – A common European Framework for ICT Professionals in all industry sectors – Part 1: Framework, 2016	C. Run – C.4. Problem Management
Gestión de problemas	Skills Framework for the Information Age V6, 2015	PBMG



Gestionar los Problemas

Componentes: Políticas y procedimientos

Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de resolución de problemas	Documenta el razonamiento y proporciona directrices para abordar los problemas que surgen de incidentes e identificar soluciones temporales validadas.	ITIL V3, 2011	Service Operation, 3. Service strategy principles



Gestionar los Problemas

Componentes: Cultura, ética y comportamiento

Elementos culturales clave	Documentación relacionada	Referencia específica
<ul style="list-style-type: none">• Respalda una cultura de gestión de problemas proactiva (detección, acción y prevención) con roles y responsabilidades claramente definidos.• Garantizar un entorno transparente y abierto para informar sobre problemas proporcionando mecanismos independientes de reporte y/o recompensas a las personas que comunican problemas.		



Gestionar los Problemas

Componentes: Servicios, infraestructura y aplicaciones

- Sistema de rastreo/resolución de problemas.



Gestionar los Problemas

Resumen de Procesos de Gestionar los Problemas

- DSS03.01 Identificar y clasificar los problemas.
- DSS03.02 Investigar y diagnosticar problemas.
- DSS03.03 Presentar los errores conocidos.
- DSS03.04 Resolver y cerrar los problemas.
- DSS03.05 Realizar una gestión proactiva de los problemas.





Gestionar los Problemas

Algunos Conceptos Clave

- **Change Management**
- La gestión del cambio es el proceso de planificar, organizar, coordinar y controlar los cambios en un sistema, como una organización, con el fin de minimizar la resistencia al cambio y lograr una transición exitosa.
- Implica identificar los cambios necesarios, comunicarlos adecuadamente a las partes interesadas y gestionar los impactos en las personas, los procesos y la tecnología dentro de una organización.
- El cambio de gestión es fundamental para implementar cambios efectivos y exitosos en cualquier entorno empresarial.





Gestionar los Problemas

Algunos Conceptos Clave

- **RFC – Request for Change**
- Una Solicitud de Cambio" es un documento utilizado en el contexto de la gestión de cambios en una organización, especialmente en el ámbito de tecnologías de la información y sistemas informáticos.
- Un RFC se utiliza para solicitar un cambio en un sistema o servicio existente.
- Puede incluir detalles como la descripción del cambio propuesto, la justificación para el cambio, el impacto esperado del cambio en el sistema o servicio, los recursos necesarios para implementar el cambio y un plan para llevar a cabo el cambio de manera efectiva.
- El RFC es un componente importante en los procesos de gestión de cambios, ya que ayuda a garantizar que los cambios se soliciten, evalúen, autoricen, implementen y documenten de manera adecuada y controlada.





Gestionar los Problemas

Algunos Conceptos Clave

- Categorización de problemas en ITIL v4.
 - **Problemas conocidos:** Son problemas que han sido identificados y documentados previamente, y para los cuales se ha desarrollado una solución o workaround (solución temporal). Estos problemas pueden surgir nuevamente en el futuro, pero se sabe cómo resolverlos.
 - **Problemas identificados:** Son problemas que han sido identificados pero que aún no se han resuelto. Estos problemas han sido registrados y están siendo investigados para encontrar una solución permanente.
 - **Problemas nuevos:** Son problemas que aún no han sido identificados o documentados. Estos problemas pueden surgir como resultado de nuevos incidentes o eventos, y necesitan ser investigados y categorizados adecuadamente.





Gestionar los Problemas

Algunos Conceptos Clave

- Clasificación de problemas del sistema, según Wim Hoogenraad.
 - **Clase A. Problema principal (Lanzamiento)**
 - Para clasificar como un problema importante hay problemas que involucran sistema no tiene mucha funcionalidad deseada.
 - En otras palabras, el sistema de información no es lo suficientemente compatible con la organización del usuario.
 - Con estos problemas, el punto de partida es que el funcionamiento del sistema de información cumple con los requisitos y deseos actuales, pero no con los futuros.
 - La característica de este tipo de problema es que los nuevos deseos a menudo se inician desde fuera de la organización del usuario.
 - Los problemas de clase A a menudo conducen a la definición de uno nuevo, del sistema de información.





Gestionar los Problemas

Algunos Conceptos Clave

- Clasificación de problemas del sistema, según Wim Hoogenraad.
 - **Clase B. Problema integral (Lanzamiento)**
 - En muchos casos, descubrimos estos problemas al evaluar la información de gestión o las desviaciones de las cifras clave.
 - Por ejemplo, parece que ciertos grupos de registros no se procesan o procesan incorrectamente.
 - Con un problema de clase B, la definición de una nueva versión del sistema de información generalmente sigue automáticamente.





Gestionar los Problemas

Algunos Conceptos Clave

- Clasificación de problemas del sistema, según Wim Hoogenraad.
 - **Clase C. Problema grave**
 - Los problemas graves se caracterizan por un estancamiento repentino en el progreso del trabajo.
 - Estos problemas se manifiestan de tal manera que la facturación o el pago ya no pueden realizarse en su totalidad o en parte; el flujo de formularios dentro de la organización se detiene total o parcialmente o el lote nocturno o diurno ya no se ejecuta total o parcialmente.
 - El momento en que ocurre uno de estos problemas determina fuertemente la gravedad.
 - Un punto de referencia importante es el momento en que debe tener lugar el procesamiento necesario en el proceso comercial principal, como la impresión de fabricar.





Gestionar los Problemas

Algunos Conceptos Clave

- Clasificación de problemas del sistema, según Wim Hoogenraad.
 - **Clase D. Problema aislado**
 - Podemos considerar los problemas aislados como problemas en el procesamiento de transacciones individuales donde encontramos que estas transacciones no se pueden procesar.
 - Por lo general, estas transacciones han ingresado falsamente en el estado incorrecto o se ha producido un "error" en el sistema.
 - Los problemas de clase D generalmente los informan los usuarios al administrador de la aplicación y pueden ser urgentes individualmente debido al interés financiero o directo involucrado en la mutación.
 - Un problema de clase D se presenta de acuerdo con un procedimiento corto.
 - Los problemas que son menos urgentes son programados por el administrador de aplicaciones como mantenimiento correctivo.





Gestionar los Problemas

Algunos Conceptos Clave

- Clasificación de problemas del sistema, según Wim Hoogenraad.
 - **Problema de optimización de clase E.**
 - Los problemas de optimización son deseos con los que el usuario suele venir espontáneamente.
 - A menudo, se trata de optimizar el trabajo en el departamento, es decir, aumentar la facilidad de uso o la eficiencia.
 - Por ejemplo, cambiar formatos de lista o integrar pantallas.
 - Los problemas de clase E generalmente no interfieren con el progreso del trabajo en el departamento, pero podrían resolver el progreso si se resuelven.
 - La agrupación con otros problemas en una versión puede tener lugar fácilmente.
 - Los procesos comerciales a menudo también juegan un papel en la evaluación de tales problemas.
 - Son principalmente los usuarios finales los que informan dichos problemas al administrador de aplicaciones funcionales.





Gestionar los Problemas

Algunos Conceptos Clave

- Clasificación de problemas del sistema, según Wim Hoogenraad.
 - **Clase F. Rendimiento**
 - Dependiendo del impacto, la gravedad de un problema de rendimiento puede variar mucho.
 - El punto de partida debe ser que el procesamiento debe realizarse dentro del tiempo especificado.
 - Podríamos clasificar los problemas de rendimiento bajo la clase E si no fuera necesario un enfoque separado.
 - Debido a que no se pueden realizar cambios funcionales en los módulos del programa debido a un problema de rendimiento, no son necesarios cambios en el diseño funcional o la organización administrativa.





Gestionar los Problemas

Algunos Conceptos Clave

- Clasificación de problemas del sistema, según Wim Hoogenraad.
 - **Clase G. Problema perturbador**
 - Los problemas molestos generalmente no tienen efecto en el procesamiento correcto de las mutaciones en el sistema de información.
 - Sin embargo, sucede que a los usuarios finales se les muestra erróneamente un mensaje en la pantalla durante su trabajo diario; que las letras pequeñas no se convierten en letras grandes o que los ceros a la izquierda se deben ingresar donde no sea necesario.
 - Debido a su importancia menor, muchos de estos problemas correctivos a menudo permanecen en los sistemas de información durante mucho tiempo, causando la molestia de los usuarios que suministran los problemas a diario.
 - Sin embargo, estos problemas fueron causados por los propios usuarios debido a una prueba de aceptación insuficientemente segura para la producción.
 - Para avanzar en la solución de estos problemas, es obvio que se agrupan con otros problemas en una versión.





Gestionar los Problemas

Algunos Conceptos Clave

- Clasificación de problemas del sistema, según Wim Hoogenraad.
 - **Clase H. Estética**
 - Los usuarios finales informan que los problemas estéticos son un problema inquietante.
 - Sin embargo, con un problema de clase H, hay un cambio de diseño deseado, como resultado de lo cual este problema de adaptación a menudo se puede resolver junto con otros problemas.





Gestionar los Problemas

Algunos Conceptos Clave

- Clasificación de problemas del sistema, según Wim Hoogenraad.
 - **Clase I. Sistémica**
 - Los problemas técnicos del sistema no serán reconocidos por la administración ni por la organización del usuario.
 - A menudo son notificados por la organización de procesamiento y a menudo se perciben como molestos, mientras que se previenen problemas futuros.
 - Los problemas de clase I generalmente trascienden un sistema de información. Como resultado, los sistemas de información individuales a menudo son secundarios a este tipo de problemas.
 - Debido a un problema de clase I, pueden ser necesarios ajustes en el sistema de información.
 - No podemos agrupar estos problemas con problemas de otras clases. Es por eso que debemos coordinar la prioridad de los problemas relacionados con el sistema con la prioridad de los otros problemas. Esto solo es posible a través de consultas mutuas entre el procesamiento y las organizaciones de usuarios.





Universidad de Santiago de Chile
Facultad de Ingeniería
Departamento de Informática

Gestión y Gobernanza TI

Ejercicio



Ejercicio

Instrucciones

- Realizaremos 3 grupos.
- Según la visión y experiencia con Operaciones TI del DIINF que tienen los miembros del grupo:
 - Grupo 1:
 - ¿Operaciones TI tiene las condiciones para alcanzar el objetivo de gestión “Gestionar las Operaciones” con un nivel de madurez 2?
 - Si no es así, mencione 3 actividades que crean las más importantes y justifique su grado de relevancia frente a las otras.
 - Grupo 2:
 - ¿Operaciones TI tiene las condiciones para alcanzar el objetivo de gestión “Gestionar las Peticiones y los Incidentes de Servicio” con un nivel de madurez 2?
 - Si no es así, mencione 3 actividades que crean las más importantes y justifique su grado de relevancia frente a las otras.
 - Grupo 3:
 - ¿Operaciones TI tiene las condiciones para alcanzar el objetivo de gestión “Gestionar los Problemas” con un nivel de madurez 2?
 - Si no es así, mencione 3 actividades que crean las más importantes y justifique su grado de relevancia frente a las otras.



Universidad de Santiago de Chile
Facultad de Ingeniería
Departamento de Informática

Gestión y Gobernanza TI

Gestionar la Continuidad



Gestionar la Continuidad

Introducción

- DSS04 – Gestionar la Continuidad.
- Pertenece al Dominio de Gestión Entregar, Dar Servicio y Soporte (DSS – Deliver, Service and Support).





Gestionar la Continuidad

Introducción

EDM01—Garantizar el establecimiento y el mantenimiento del marco de gobierno

EDM02—Asegurar la realización de beneficios

EDM03—Asegurar la optimización del riesgo

EDM04—Asegurar la optimización de los recursos

EDM05—Asegurar la transparencia de las partes interesadas

APO01—Gestionar el marco de gestión de TI

APO02—Gestionar la estrategia

APO03—Gestionar la arquitectura de la empresa

APO04—Gestionar la innovación

APO05—Gestionar el portafolio

APO06—Gestionar el presupuesto y los costes

APO07—Gestionar los recursos humanos

APO08—Gestionar las relaciones

APO09—Gestionar los acuerdos de servicio

APO10—Gestionar los proveedores

APO11—Gestionar la calidad

APO12—Gestionar el riesgo

APO13—Gestionar la seguridad

APO14—Gestionar los datos

MEA01—Gestionar la monitorización del rendimiento y la conformidad

BAI01—Gestionar los programas

BAI02—Gestionar la definición de requisitos

BAI03—Gestionar la identificación y construcción de soluciones

BAI04—Gestionar la disponibilidad y capacidad

BAI05—Gestionar los cambios organizativos

BAI06—Gestionar los cambios de TI

BAI07—Gestionar la aceptación y la transición de los cambios de TI

MEA02—Gestionar el sistema de control interno

BAI08—Gestionar el conocimiento

BAI09—Gestionar los activos

BAI10—Gestionar la configuración

BAI11—Gestionar los proyectos

MEA03—Gestionar el cumplimiento de los requisitos externos

DSS01—Gestionar las operaciones

DSS02—Gestionar las solicitudes e incidentes de servicio

DSS03—Gestionar los problemas

DSS04—Gestionar la continuidad

DSS05—Gestionar los servicios de seguridad

DSS06—Gestionar los controles de procesos de negocio

MEA04—Gestionar el aseguramiento

Entregar, Dar Servicio y Soporte (DSS – Deliver, Service and Support)



Gestionar la Continuidad

Descripción

- Establecer y mantener un plan que permita a las organizaciones empresariales y a TI responder a los incidentes y adaptarse rápidamente a las interrupciones.
- Esto permitirá la operación continua de los procesos críticos de negocio y de los servicios de I&T necesarios, y mantener la disponibilidad de recursos, activos e información en un nivel aceptable para la empresa.





Gestionar la Continuidad

Propósito

- Adaptarse rápidamente, continuar con las operaciones del negocio y mantener la disponibilidad de los recursos y la información a un nivel aceptable para la empresa en caso de una interrupción significativa (p.ej., amenazas, oportunidades, demandas).





Gestionar la Continuidad

Componentes


- Procesos (8):
 - DSS04.01 Definir la política de continuidad del negocio, sus objetivos y alcance.
 - DSS04.02 Mantener la resiliencia del negocio.
 - DSS04.03 Desarrollar e implementar una respuesta de continuidad del negocio.
 - DSS04.04 Realizar ejercicios, probar y revisar el plan de continuidad del negocio (BCP) y el plan de respuesta ante desastres (DRP).
 - DSS04.05 Revisar, mantener y mejorar los planes de continuidad.
 - DSS04.06 Realizar formación sobre el plan de continuidad.
 - DSS04.07 Administrar los acuerdos de respaldo.
 - DSS04.08 Realizar revisiones post-reanudación.
- Estructuras organizativas.
- Flujos y elementos de información.
- Personas, habilidades y competencias (1).
- Políticas y procedimientos (2).
- Cultura, ética y comportamiento (1).
- Servicios, infraestructura y aplicaciones (3).





Gestionar la Continuidad


El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:

Metas Empresariales			Metas de Alineamiento	
<ul style="list-style-type: none">• EG01 Portafolio de productos y servicios competitivos• EG02 Gestión de riesgo de negocio• EG06 Continuidad y disponibilidad del servicio del negocio• EG08 Optimización de la funcionalidad del proceso interno de negocio			<ul style="list-style-type: none">• AG05 Prestación de servicios de I&T conforme a los requisitos de negocio• AG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad	
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento	
EG01	<ul style="list-style-type: none">• Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercado• Porcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del cliente• Porcentaje de productos y servicios que proporcionan una ventaja competitiva• Plazo de comercialización para nuevos productos y servicios		AG05	<ul style="list-style-type: none">• Porcentaje de partes interesadas del negocio satisfechas con que la prestación de servicios de I&T cumpla con los niveles de servicio acordados• Número de interrupciones del negocio debido a incidentes de servicios de I&T• Porcentaje de usuarios satisfechos con la calidad de la prestación de servicios de I&T
EG02	<ul style="list-style-type: none">• Porcentaje de objetivos y servicios empresariales críticos cubiertos por la evaluación de riesgos• Proporción de incidentes significativos que no se identificaron en la evaluación de riesgos frente al total de incidentes• Frecuencia de actualización del perfil de riesgo			



Gestionar la Continuidad

El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:

Metas Empresariales			Metas de Alineamiento	
<ul style="list-style-type: none">EG01 Portafolio de productos y servicios competitivosEG02 Gestión de riesgo de negocioEG06 Continuidad y disponibilidad del servicio del negocioEG08 Optimización de la funcionalidad del proceso interno de negocio			<ul style="list-style-type: none">AG05 Prestación de servicios de I&T conforme a los requisitos de negocioAG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad	
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento	
EG06	<ul style="list-style-type: none">Número de interrupciones del servicio al cliente o procesos del negocio que han causado incidentes significativosCoste de los incidentes para el negocioNúmero de horas de procesamiento perdidas en el negocio debido a interrupciones inesperadas del servicioPorcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados		AG07	<ul style="list-style-type: none">Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o descrédito públicoNúmero de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito públicoNúmero de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o descrédito público
EG08	<ul style="list-style-type: none">Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso de negocioNiveles de satisfacción de los clientes con las capacidades de prestación de serviciosNiveles de satisfacción de los proveedores con las capacidades de la cadena de suministro			



Gestionar la Continuidad

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS04.01 Definir la política de continuidad del negocio, sus objetivos y alcance. Definir la política y alcance de la continuidad del negocio, alineado con los objetivos de la empresa y de las partes interesadas, para mejorar la resiliencia del negocio.	<ul style="list-style-type: none">• Porcentaje de objetivos y alcance de continuidad del negocio reprocesados debido a procesos y actividades no identificados• Porcentaje de partes interesadas clave que participan, definen y acuerdan la política y el alcance de continuidad	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">• Identificar procesos de negocio y actividades de servicio internos y externalizados que son críticos para las operaciones empresariales o necesarios para satisfacer las obligaciones legales y/o contractuales.		2
<ul style="list-style-type: none">• Identificar partes interesadas clave y los roles y responsabilidades para definir y acordar la política y el alcance de continuidad.		
<ul style="list-style-type: none">• Definir y documentar los objetivos de política mínimos acordados y el alcance de la resiliencia del negocio.		
<ul style="list-style-type: none">• Identificar procesos de negocio de soporte esenciales y servicios de I&T relacionados.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
HITRUST CSF versión 9, septiembre de 2017		12.01 Information Security Aspects of Business Continuity Management
ISF, The Standard of Good Practice for Information Security 2016		BC1.1 Business Continuity Strategy; BC1.2 Business Continuity Programme
ISO/IEC 27002:2013/Cor.2:2015(E)		17. Aspectos de seguridad de la información de la gestión de la continuidad del negocio
National Institute of Standards and Technology Special Publication 800–53, Revisión 5 (Borrador), agosto de 2017		3.6 Contingency planning (CP–1)



Gestionar la Continuidad

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS04.02 Mantener la resiliencia del negocio. Evaluar las opciones de resiliencia del negocio y elegir una estrategia viable y rentable para asegurar la continuidad, la recuperación ante un desastre y la respuesta ante incidentes de la empresa ante un desastre u otro incidente o interrupción mayor.	<ul style="list-style-type: none">• Inactividad total derivada de un incidente o interrupción importante.• Porcentaje de partes interesadas claves involucradas en el análisis de impacto del negocio que evalúan el impacto a lo largo del tiempo de duración de una interrupción de funciones críticas del negocio y el efecto que una interrupción tendría sobre ellas	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">• Identificar escenarios potenciales que podrían ocasionar eventos que darían lugar a incidentes disruptivos significativos.		2
<ul style="list-style-type: none">• Conducir un análisis de impacto del negocio para evaluar el impacto a lo largo del tiempo de duración de una disrupción de funciones críticas del negocio y el efecto que una interrupción tendría en ellas.		
<ul style="list-style-type: none">• Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y el entorno de I&T que lo soporta, conforme a una duración aceptable de interrupción del negocio y la suspensión tolerable máxima.		
<ul style="list-style-type: none">• Determinar las condiciones y los dueños de las decisiones clave que ocasionarán que se invoquen los planes de continuidad.		
<ul style="list-style-type: none">• Evaluar la probabilidad de amenazas que pudieran causar la pérdida de la continuidad del negocio.• Identificar medidas que reducirán la probabilidad y el impacto a través de una mejor prevención y una mayor resiliencia.		3
<ul style="list-style-type: none">• Analizar requisitos de continuidad para identificar posibles opciones estratégicas empresariales y técnicas.		
<ul style="list-style-type: none">• Identificar los requisitos y costes de recursos para cada opción técnica estratégica y realizar recomendaciones estratégicas.		
<ul style="list-style-type: none">• Obtener la aprobación de ejecutivos del negocio para las opciones estratégicas seleccionadas.		



Gestionar la Continuidad

Componente: Procesos

Práctica de Gestión	Métricas Modelo
DSS04.02 Mantener la resiliencia del negocio. Evaluar las opciones de resiliencia del negocio y elegir una estrategia viable y rentable para asegurar la continuidad, la recuperación ante un desastre y la respuesta ante incidentes de la empresa ante un desastre u otro incidente o interrupción mayor.	<ul style="list-style-type: none">• Inactividad total derivada de un incidente o interrupción importante.• Porcentaje de partes interesadas claves involucradas en el análisis de impacto del negocio que evalúan el impacto a lo largo del tiempo de duración de una interrupción de funciones críticas del negocio y el efecto que una interrupción tendría sobre ellas
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
ISF, The Standard of Good Practice for Information Security 2016	BC1.3 Resilient Technical Environments
ITIL V3, 2011	Service Design, 4.6 IT Continuity Management
National Institute of Standards and Technology Special Publication 800–53, Revisión 5 (Borrador), agosto de 2017	3.6 Contingency planning (CP–2)



Gestionar la Continuidad

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS04.03 Desarrollar e implementar una respuesta de continuidad del negocio. <ul style="list-style-type: none">Desarrollar un plan de continuidad del negocio (BCP) y un plan de recuperación de desastres (DRP) basados en la estrategia.Documentar todos los procedimientos necesarios para que la empresa continúe con sus actividades críticas en caso de incidente.	<ul style="list-style-type: none">Número de sistemas críticos de negocio no cubiertos por el planPorcentaje de partes interesadas claves involucradas en el desarrollo de BCPs y DRPs	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">Definir acciones y comunicaciones de respuesta a incidentes que se deban tomar en caso de interrupción.Definir roles y responsabilidades relacionados, incluida la rendición de cuentas para la política y la implementación.		2
<ul style="list-style-type: none">Garantizar que los proveedores clave y socios externalizados cuenten con planes de continuidad efectivos.Obtener evidencia auditada según se requiera.		
<ul style="list-style-type: none">Definir las condiciones y los procedimientos de recuperación que permitirán la reanudación del procesamiento de negocio.Incluir la actualización y sincronización de bases de datos para preservar la integridad de la información.		
<ul style="list-style-type: none">Desarrollar y mantener BCPs y DRPs operativos que contengan los procedimientos a seguir para permitir el funcionamiento continuo de procesos de negocio críticos y/o acuerdos de procesamiento temporales.Incluir vínculos a los planes de proveedores de servicios externalizados.		
<ul style="list-style-type: none">Definir y documentar los recursos requeridos para respaldar los procedimientos de continuidad y recuperación, teniendo en cuenta las personas, las instalaciones y la infraestructura de TI.		
<ul style="list-style-type: none">Definir y documentar los requisitos de copias de seguridad de la información necesarios para respaldar los planes.Incluir planes y documentos en papel, así como archivos de datos.Considerar la necesidad de seguridad y almacenamiento fuera de las instalaciones.		
<ul style="list-style-type: none">Determinar las habilidades requeridas para los individuos involucrados en la ejecución del plan y los procedimientos.		



Gestionar la Continuidad

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS04.03 Desarrollar e implementar una respuesta de continuidad del negocio. <ul style="list-style-type: none">Desarrollar un plan de continuidad del negocio (BCP) y un plan de recuperación de desastres (DRP) basados en la estrategia.Documentar todos los procedimientos necesarios para que la empresa continúe con sus actividades críticas en caso de incidente.	<ul style="list-style-type: none">Número de sistemas críticos de negocio no cubiertos por el planPorcentaje de partes interesadas claves involucradas en el desarrollo de BCPs y DRPs	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">Distribuir los planes y la documentación soporte de forma segura a las partes interesadas debidamente autorizadas.Asegurar que los planes y la documentación son accesibles en todos los escenarios de desastre.		3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISF, The Standard of Good Practice for Information Security 2016		BC1.4 Crisis Management; BC2.1 Business Continuity Planning
National Institute of Standards and Technology Special Publication 800–53, Revisión 5 (Borrador), agosto de 2017		3.6 Contingency planning (CP–6, CP–9, CP–10)



Gestionar la Continuidad

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS04.04 Realizar ejercicios, probar y revisar el plan de continuidad del negocio (BCP) y el plan de respuesta ante desastres (DRP). Probar la continuidad de forma periódica para ver el comportamiento de los planes contra resultados predeterminados, mantener la resiliencia del negocio y permitir que se desarrollen soluciones innovadoras.	<ul style="list-style-type: none">• Frecuencia de las pruebas• Número de ejercicios y pruebas que alcanzaron los objetivos de recuperación	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">• Definir objetivos para ejercitar y probar los sistemas del negocio, técnicos, logísticos, administrativos, procedimentales y operativos del plan para verificar la integridad de los BCP y DRP en el cumplimiento del riesgo del negocio.		2
<ul style="list-style-type: none">• Definir y acordar ejercicios con las partes interesadas que sean realistas y validen los procedimientos de continuidad.• Incluir roles y responsabilidades y acuerdos de retención de datos que causen la mínima disrupción a los procesos del negocio.		
<ul style="list-style-type: none">• Asignar roles y responsabilidades para la ejecución de ejercicios y pruebas del plan de continuidad.		
<ul style="list-style-type: none">• Programar ejercicios y actividades de prueba de acuerdo a lo definido en los planes de continuidad.		3
<ul style="list-style-type: none">• Llevar a cabo una sesión informativa y un análisis luego del ejercicio para considerar lo alcanzado.		4
<ul style="list-style-type: none">• De acuerdo a los resultados de la revisión, desarrollar recomendaciones para mejorar los planes de continuidad actuales.		5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
CMMI Cybermaturity Platform, 2018		PP.RS Develop and Maintain Response Plans; PP.RP Develop and Maintain Recovery Plans
ISF, The Standard of Good Practice for Information Security 2016		BC2.3 Business Continuity Testing
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, Agosto de 2016		CSC 20: Penetration Tests and Red Team Exercises



Gestionar la Continuidad

Componente: Procesos

Práctica de Gestión	Métricas Modelo		
DSS04.05 Revisar, mantener y mejorar los planes de continuidad. <ul style="list-style-type: none">Conducir una revisión periódica de la capacidad de continuidad para asegurar su idoneidad, lo adecuado y su efectividad.Gestionar los cambios a los planes de acuerdo con el proceso de control de cambios para asegurar que los planes de continuidad se mantienen actualizados y reflejan continuamente los requisitos actuales del negocio.	<ul style="list-style-type: none">Porcentaje de mejoras acordadas para el plan que se han incorporado al planPorcentaje de planes de continuidad y evaluaciones del impacto en el negocio que se encuentran actualizados		
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">Revisar regularmente los planes de continuidad y la capacidad contra las hipótesis consideradas y los objetivos estratégicos y operativos actuales del negocio.			3
<ul style="list-style-type: none">Revisar de forma regular los planes de continuidad para considerar el impacto de cambios nuevos o mayores en la organización empresarial, procesos de negocio, acuerdos con terceros, tecnologías, infraestructura, sistemas operativos y sistemas de aplicación.			
<ul style="list-style-type: none">Considerar si pudiera necesitarse revisar la evaluación de impacto del negocio, dependiendo de la naturaleza del cambio.			
<ul style="list-style-type: none">Recomendar cambios en la política, los planes, procedimientos, infraestructura y roles y responsabilidades.Comunicarlos como adecuados para la aprobación por la dirección y el procesamiento a través del proceso de gestión de cambios de TI.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin Documentación relacionada para esta práctica de gestión			



Gestionar la Continuidad

Componente: Procesos

Práctica de Gestión		Métricas Modelo	
DSS04.06 Realizar formación sobre el plan de continuidad. Proporcionar sesiones periódicas de formación sobre los procedimientos y sus roles y responsabilidades en caso de interrupción a todas las partes internas y externas involucradas.		<ul style="list-style-type: none">• Porcentaje de partes interesadas internas y externas que han recibido capacitación• Porcentaje de partes internas y externas relevantes cuyas habilidades y competencias se encuentran actualizadas	
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">• Realizar formación y concienciación sobre el BCP y el DRP			2
<ul style="list-style-type: none">• Definir y mantener los requisitos y planes de formación para aquellas personas que realizan planificación de continuidad, evaluaciones de impacto, evaluaciones de riesgo, comunicación con medios de comunicación y respuesta a incidentes.• Asegurar que los planes de formación consideren la frecuencia de capacitación y los mecanismos de prestación de la formación.			3
<ul style="list-style-type: none">• Desarrollar competencias basadas en formación práctica, incluida la participación en ejercicios y pruebas.			
<ul style="list-style-type: none">• De acuerdo a los resultados de los ejercicios y las pruebas, supervisar habilidades y competencias.			4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
National Institute of Standards and Technology Special Publication 800–53, Revisión 5 (Borrador), agosto de 2017		3.6 Contingency planning (CP–4)	



Gestionar la Continuidad

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS04.07 Administrar los acuerdos de respaldo. Mantener la disponibilidad de la información crítica para el negocio.	<ul style="list-style-type: none">• Porcentaje de medios de respaldo transferidos y almacenados de forma segura• Porcentaje de restauración exitosa y oportuna de copias de seguridad o copias de medios alternativos	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">• Hacer una copia de seguridad de los sistemas, aplicaciones, datos y documentación conforme a un calendario definido.• Considerar una frecuencia (mensual, semanal, diario, etc.), modo de copia de seguridad (ej. disk mirroring para copias de seguridad en tiempo real frente a DVD–ROM para retención a largo plazo), tipo de copia de seguridad (p.ej., completa vs. incremental), y tipo de medios.• Considerar también copias de seguridad online automatizadas, tipos de datos (p. ej. voz, ópticos), creación de logs, datos críticos de computación de usuario final (ej. hojas de cálculo), ubicación física y lógica de las fuentes de datos, derechos de acceso y seguridad, y encriptación.		2
<ul style="list-style-type: none">• Definir requisitos para el almacenamiento en las instalaciones (on–site) y fuera de ellas (off–site) de copias de seguridad de datos, conforme a los requisitos de negocio.• Considerar el acceso requerido para hacer copias de seguridad de los datos.		
<ul style="list-style-type: none">• Probar y refrescar de forma periódica los datos archivados y las copias de seguridad de los datos.		
<ul style="list-style-type: none">• Garantizar que se haga una copia de seguridad o se aseguren de forma adecuada los sistemas, aplicaciones, datos y documentación mantenida o procesada por terceros.• Considerar que se requiera que los terceros devuelvan las copias de seguridad.• Considerar la opción de mantenimiento en fiducia (escrow, por su término en inglés) o acuerdos de depósitos.		



Gestionar la Continuidad

Componente: Procesos

Práctica de Gestión	Métricas Modelo
DSS04.07 Administrar los acuerdos de respaldo. Mantener la disponibilidad de la información crítica para el negocio.	<ul style="list-style-type: none">• Porcentaje de medios de respaldo transferidos y almacenados de forma segura• Porcentaje de restauración exitosa y oportuna de copias de seguridad o copias de medios alternativos
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Cybermaturity Platform, 2018	IP.BP Apply Backup Processes
HITRUST CSF versión 9, septiembre de 2017	09.05 Information Back-Up
ISF, The Standard of Good Practice for Information Security 2016	SY2.3 Backup
ISO/IEC 27002:2013/Cor.2:2015(E)	12.3 Backup
National Institute of Standards and Technology Special Publication 800–53, Revisión 5 (Borrador), agosto de 2017	3.6 Contingency planning (CP–3)
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, Agosto de 2016	CSC 10: Data Recovery Capability



Gestionar la Continuidad

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS04.08 Realizar revisiones post–reanudación. Evaluar la idoneidad del plan de continuidad del negocio (BCP) y el plan de respuesta ante desastres (DRP) tras la reanudación exitosa de los procesos y servicios del negocio después de una interrupción.	<ul style="list-style-type: none">• Porcentaje de problemas identificados que se han abordado posteriormente en el plan• Porcentaje de problemas identificados que se han abordado posteriormente en los materiales de formación	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">• Evaluar el cumplimiento de los BCP y DRP documentados.		4
<ul style="list-style-type: none">• Determinar la efectividad de los planes, capacidades de continuidad, roles y responsabilidades, habilidades y competencias, resiliencia a incidentes, infraestructura técnica y estructuras organizativas y relaciones.		
<ul style="list-style-type: none">• Identificar las debilidades u omisiones en los planes y capacidades y realizar recomendaciones de mejora.• Obtener la aprobación de la dirección para cualquier cambio en los planes y aplicarlos a través del proceso de control de cambios de la empresa.		5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
Sin documentación relacionada para esta práctica de gestión		



Práctica clave de gestión



Gestionar la Continuidad

Componentes: Flujos y elementos de información

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS04.01 Definir la política de continuidad del negocio, sus objetivos y alcance.	APO09.03	SLAs	Política y objetivos para la continuidad del negocio	APO01.02
			Evaluaciones de capacidades y brechas de continuidad actuales	Interna
			Escenarios de incidentes disruptivos	Interna
DSS04.02 Mantener la resiliencia del negocio.	APO12.06	<ul style="list-style-type: none">Comunicación de impacto del riesgoCausas raíz relacionadas con riesgos	Opciones estratégicas aprobadas	APO02.05
			BIAs	APO12.02
			Requisitos de continuidad	Interna
DSS04.03 Desarrollar e implementar una respuesta de continuidad del negocio.	APO09.03	OLAs	Acciones y comunicaciones para respuesta a incidentes	DSS02.01
			BCP	Interna
DSS04.04 Realizar ejercicios, probar y revisar el plan de continuidad del negocio (BCP) y el plan de respuesta ante desastres (DRP).			Resultados y recomendaciones de pruebas	Interna
			Ejercicios de prueba	Interna
			Objetivos de la prueba	Interna



Gestionar la Continuidad

Componentes: Flujos y elementos de información

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS04.05 Revisar, mantener y mejorar los planes de continuidad.			Cambios recomendados a los planes	Interna
			Resultados de revisiones de planes	Interna
DSS04.06 Realizar formación sobre el plan de continuidad.	Recursos Humanos	Lista de personal que necesita formación	Supervisión de resultados de habilidades y competencias.	APO07.03
			Requisitos de formación	APO07.03
DSS04.07 Administrar los acuerdos de copia de seguridad.	APO14.10	<ul style="list-style-type: none">Plan de copias de seguridadPlan de pruebas de copias de seguridad	Probar los resultados de las copias de seguridad de los datos	Interna
			Copia de seguridad de los datos	Interna; APO14.08
DSS04.08 Realizar revisiones post–reanudación.			Cambios aprobados a los planes	BAI06.01
			Informe de la revisión post–reanudación.	Interna
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)			Referencia específica	
Sin documentación relacionada para este componente.				



Gestionar la Continuidad

Componentes: Personas, habilidades y competencias

Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Gestión de la continuidad	Skills Framework for the Information Age V6, 2015	COPL



Gestionar la Continuidad

Componentes: Políticas y procedimientos

Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de continuidad del negocio (BCP)	<ul style="list-style-type: none">Señala el compromiso de la dirección con la evaluación de impacto del negocio (BIA), el plan de contingencia del negocio (incluida la recuperación confiable), los requisitos de recuperación para sistemas críticos, umbrales y disparadores de las contingencias definidos, plan de escalamiento, plan de recuperación de datos, formación y pruebas.		
Política de gestión de crisis	<ul style="list-style-type: none">Establece las directrices y la secuencia de la respuesta ante crisis en áreas clave del riesgo.La gestión de crisis es, junto con la seguridad de I&T, la gestión de red, y la seguridad de los datos y la privacidad, una de las políticas a nivel operativo que debería considerarse para una gestión de riesgos de I&T completa.		



Gestionar la Continuidad

Componentes: Cultura, ética y comportamiento

Elementos culturales clave	Documentación relacionada	Referencia específica
<ul style="list-style-type: none">• Integrar la necesidad de resiliencia de negocio en la cultura empresarial.• Informar de forma regular y frecuente a los empleados sobre los valores fundamentales, comportamientos deseados y objetivos estratégicos para conservar la compostura e imagen empresarial en cualquier situación.• Probar de forma regular los procedimientos de continuidad y la recuperación de desastres.		



Gestionar la Continuidad

Componentes: Servicios, infraestructura y aplicaciones

- Servicios externos de hosting.
- Herramientas de monitorización de incidentes.
- Servicios de instalaciones para almacenamiento remoto.



Gestionar la Continuidad

Resumen de Procesos de Gestionar la Continuidad

- DSS04.01 Definir la política de continuidad del negocio, sus objetivos y alcance.
- DSS04.02 Mantener la resiliencia del negocio.
- DSS04.03 Desarrollar e implementar una respuesta de continuidad del negocio.
- DSS04.04 Realizar ejercicios, probar y revisar el plan de continuidad del negocio (BCP) y el plan de respuesta ante desastres (DRP).
- DSS04.05 Revisar, mantener y mejorar los planes de continuidad.
- DSS04.06 Realizar formación sobre el plan de continuidad.
- DSS04.07 Administrar los acuerdos de respaldo.
- DSS04.08 Realizar revisiones post-reanudación.





Gestionar la Continuidad

Algunos Conceptos Clave

- **BIA – Business Impact Analysis:**
- El Análisis de Impacto en el Negocio es una actividad clave en la gestión de la continuidad del negocio (BCM, por sus siglas en inglés). El objetivo del BIA es identificar y evaluar el impacto potencial de la interrupción de los procesos de negocio en una organización.
- Durante el BIA, se analizan los procesos de negocio críticos, identificando sus componentes clave, como personas, tecnología, información y proveedores. Se evalúa el impacto que tendría la interrupción de estos procesos en términos de pérdida financiera, daño a la reputación, incumplimiento de regulaciones, entre otros.
- El BIA ayuda a las organizaciones a priorizar sus esfuerzos de continuidad del negocio, identificando los procesos críticos que deben ser restaurados primero en caso de interrupción. También proporciona información valiosa para desarrollar estrategias de recuperación y planes de continuidad del negocio efectivos.





Gestionar la Continuidad

Algunos Conceptos Clave

- **BCP – Business Continuity Plan:**
- El Planificación de la Continuidad del Negocio es el proceso de crear sistemas de prevención y recuperación para manejar posibles amenazas a una organización. El objetivo principal del BCP es garantizar que una organización pueda continuar operando durante y después de un desastre o interrupción.
- El BCP incluye la identificación de amenazas potenciales y sus impactos en las operaciones de la organización, la evaluación de la vulnerabilidad de la organización a estas amenazas y la creación de planes y estrategias para minimizar el impacto de los desastres y asegurar la continuidad de las operaciones.
- Los planes de continuidad del negocio generalmente incluyen medidas preventivas, como la implementación de sistemas de respaldo y redundancia, así como procedimientos de respuesta, como la activación de equipos de respuesta a emergencias y la comunicación con empleados, clientes y proveedores durante una crisis.





Gestionar la Continuidad

Algunos Conceptos Clave

- **DRP – Disaster Recovery Plan:**
- La Planificación de la Recuperación de Desastres es el proceso de crear un enfoque detallado para la recuperación de sistemas, aplicaciones y datos después de un desastre o interrupción grave. El objetivo del DRP es minimizar el tiempo de inactividad y restaurar las operaciones normales de la organización en el menor tiempo posible después de un desastre.
- El DRP incluye la identificación de los sistemas y datos críticos para las operaciones de la organización, la evaluación de los riesgos y amenazas que podrían afectar a estos sistemas y datos, y la creación de planes detallados para la recuperación después de un desastre. Esto puede incluir la implementación de procedimientos de copia de seguridad y restauración, la asignación de responsabilidades para la recuperación y la coordinación con proveedores y socios comerciales clave.
- Los planes de recuperación de desastres suelen incluir pruebas y ejercicios periódicos para garantizar que estén actualizados y sean efectivos en caso de un desastre real.





Gestionar la Continuidad

Algunos Conceptos Clave

- **RTO – Recovery Time Objective**
- El Objetivo de Tiempo de Recuperación se refiere a la cantidad máxima de tiempo que una organización puede permitirse que transcurra entre una interrupción de sus operaciones y su recuperación.
- Establece cuánto tiempo máximo una empresa puede estar sin un servicio o función específica antes de que comiencen a surgir consecuencias graves.
- Es un componente importante de la planificación de la continuidad del negocio y de los planes de recuperación ante desastres, ya que ayuda a definir los límites de tiempo dentro de los cuales deben realizarse las acciones de recuperación para minimizar el impacto de una interrupción.





Gestionar la Continuidad

Algunos Conceptos Clave

- **RPO – Recovery Point Objective**
- El Objetivo de Punto de Recuperación se refiere al punto en el tiempo al que una organización desea recuperar sus datos en caso de una interrupción o desastre.
- Establece la cantidad máxima de tiempo durante la cual los datos pueden perderse en el caso de una interrupción antes de que el impacto sea considerado inaceptable.
- Por ejemplo, si una organización tiene un RPO de una hora, significa que está dispuesta a perder como máximo una hora de datos en caso de un evento catastrófico.
- Es un componente crítico de la planificación de la continuidad del negocio y la recuperación ante desastres, ya que ayuda a determinar con qué frecuencia se deben realizar copias de seguridad y cuántos datos se pueden perder en caso de una interrupción.





Gestionar la Continuidad

Algunos Conceptos Clave

- **WRT – Tiempo de Recuperación del Trabajo**
- El Tiempo de Recuperación del Trabajo se refiere al tiempo que tiempo en el que se recuperará el servicio real, mediante la verificación de los sistemas y la puesta en línea de estos.

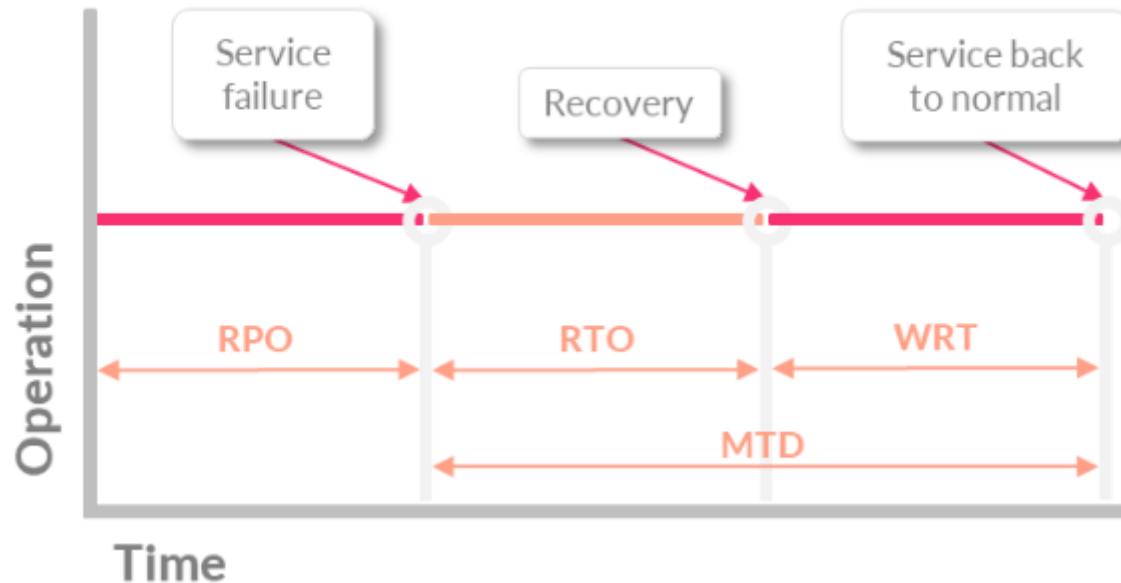




Gestionar la Continuidad

Algunos Conceptos Clave

- RPO, RTO, MTD y WRT





Universidad de Santiago de Chile
Facultad de Ingeniería
Departamento de Informática

Gestión y Gobernanza TI

Gestionar los Servicios de
Seguridad



Gestionar los Servicios de Seguridad

Introducción

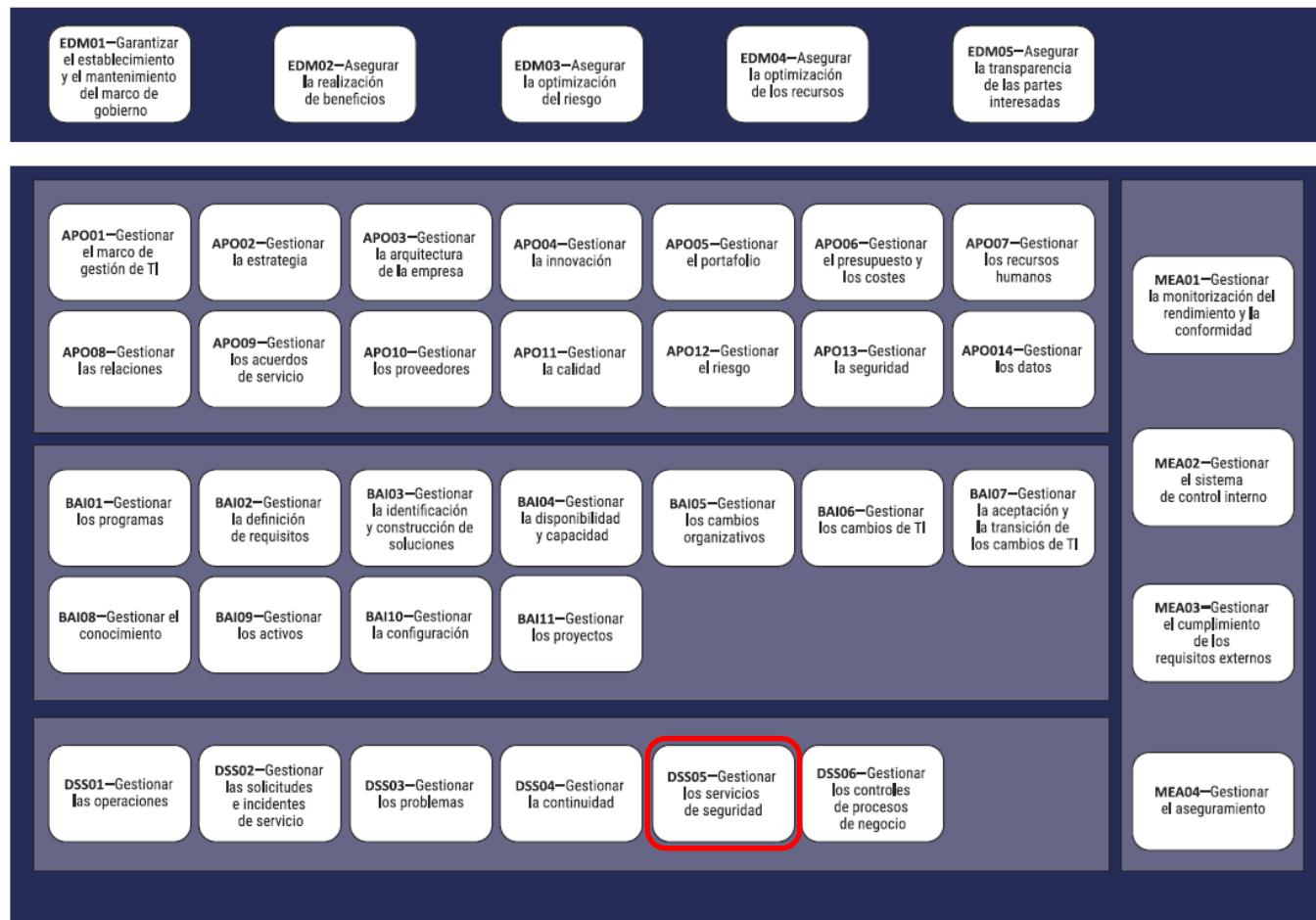
- DSS05 – Gestionar los Servicios de Seguridad.
- Pertenece al Dominio de Gestión Entregar, Dar Servicio y Soporte (DSS – Deliver, Service and Support).





Gestionar los Servicios de Seguridad

Introducción



Entregar, Dar Servicio y Soporte (DSS – Deliver, Service and Support)



Gestionar los Servicios de Seguridad

Descripción

- Proteger la información de la empresa para mantener el nivel de riesgo de la seguridad de la información aceptable para la empresa, conforme con la política de seguridad.
- Establecer y mantener roles y privilegios de acceso de seguridad de la información.
- Realizar una monitorización de la seguridad.





Gestionar los Servicios de Seguridad

Propósito

- Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad de la información





Gestionar la Continuidad

Componentes


- Procesos (7):
 - DSS05.01 Proteger contra software malicioso.
 - DSS05.02 Gestionar la seguridad de la conectividad y de la red.
 - DSS05.03 Gestionar la seguridad de endpoint.
 - DSS05.04: Gestionar la identidad del usuario y el acceso lógico.
 - DSS05.05 Gestionar el acceso físico a los activos de I&T.
 - DSS05.06: Gestionar documentos sensibles y dispositivos de salida.
 - DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad.
- Estructuras organizativas.
- Flujos y elementos de información.
- Personas, habilidades y competencias (4).
- Políticas y procedimientos (1).
- Cultura, ética y comportamiento (1).
- Servicios, infraestructura y aplicaciones (8).





Gestionar los Servicios de Seguridad

El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:

Metas Empresariales			Metas de Alineamiento	
<ul style="list-style-type: none">EG02 – Gestión de riesgo del negocioEG06 – Continuidad y disponibilidad del servicio del negocio			<ul style="list-style-type: none">AG02 Gestión de riesgo relacionado con I&TAG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad	
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento	
EG02	<ul style="list-style-type: none">Porcentaje de objetivos y servicios empresariales críticos cubiertos por la evaluación de riesgosNúmero de incidentes significativos que no se identificaron en la evaluación de riesgos frente al total de incidentesFrecuencia de actualización del perfil de riesgo		AG02	<ul style="list-style-type: none">Frecuencia de actualización del perfil de riesgoPorcentaje de evaluaciones de riesgo empresarial que incluyen el riesgo relacionado con I&TNúmero de incidentes significativos relacionados con I&T que no se identificaron en la evaluación de riesgos
EG06	<ul style="list-style-type: none">Número de interrupciones del servicio al cliente o procesos empresariales que causan incidentes significativosCoste de los incidentes para el negocioNúmero de horas de procesamiento perdidas en el negocio debido a interrupciones no planificadas del servicioPorcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados		AG07	<ul style="list-style-type: none">Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o descrédito públicoNúmero de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito públicoNúmero de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o descrédito público



Gestionar los Servicios de Seguridad

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS05.01 Proteger contra software malicioso Implementar y mantener en toda la empresa medidas preventivas, detectivas y correctivas (especialmente parches de seguridad y control de virus actualizados) para proteger los sistemas de información y la tecnología del software malicioso (ej. ransomware, malware, virus, gusanos, spyware y spam).	<ul style="list-style-type: none">• Número de ataques exitosos de software malicioso• Porcentaje de empleados que no pasan las pruebas de ataques maliciosos (ej. la prueba de correos electrónicos de phishing)	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">• Instalar y activar herramientas de protección contra software malicioso en todas las instalaciones de procesamiento, con archivos de definición de software malicioso que se actualizan según sea necesario (automáticamente o semiautomáticamente)		2
<ul style="list-style-type: none">• Filtrar el tráfico de entrada, como el correo electrónico y las descargas, para protegerlo de información no solicitada (ej. spyware, correos electrónicos de phishing).		
<ul style="list-style-type: none">• Comunicar acerca de concienciación sobre software malicioso y hacer cumplir los procedimientos y responsabilidades de prevención.• Impartir formación periódica sobre malware en el uso de correo electrónico e Internet.• Formar a los usuarios para que no abran e informen sobre correos electrónicos sospechosos y no instalen software compartido o no aprobado.		3
<ul style="list-style-type: none">• Distribuir todo el software de protección centralmente (versión y parches) usando una configuración centralizada y la gestión de cambios de TI.		
<ul style="list-style-type: none">• Revisar y evaluar la información sobre nuevas amenazas potenciales (ej. revisión de los consejos de seguridad de productos y servicios de proveedores) de forma regular.		4



Gestionar los Servicios de Seguridad

Componente: Procesos

Práctica de Gestión	Métricas Modelo
DSS05.01 Proteger contra software malicioso Implementar y mantener en toda la empresa medidas preventivas, detectivas y correctivas (especialmente parches de seguridad y control de virus actualizados) para proteger los sistemas de información y la tecnología del software malicioso (ej. ransomware, malware, virus, gusanos, spyware y spam).	<ul style="list-style-type: none">Número de ataques exitosos de software maliciosoPorcentaje de empleados que no pasan las pruebas de ataques maliciosos (ej. la prueba de correos electrónicos de phishing)
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Cybermaturity Platform, 2018	DP.DC Detect Malicious Code; RI.VT Vulnerability and Threat Identification
HITRUST CSF versión 9, septiembre de 2017	09.04 Protection Against Malicious & Mobile Code
SF, The Standard of Good Practice for Information Security 2016	TS1 Security Solutions
SO/IEC 27002:2013/Cor.2:2015(E)	12.2 Protection against malware
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, Agosto de 2016	CSC 4: Continuous Vulnerability Assessment and Remediation; CSC 8: Malware Defenses



Gestionar los Servicios de Seguridad

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS05.02 Gestionar la seguridad de la conectividad y de la red. Usar medidas de seguridad y procedimientos de gestión relacionados para proteger la información a través de todos los métodos de conectividad.	<ul style="list-style-type: none">• Número de brechas del firewall• Número de vulnerabilidades descubiertas• Porcentaje de tiempo que la red y los sistemas no están disponibles debido a incidentes de seguridad	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">• Permitir que solo los dispositivos autorizados tengan acceso a la información corporativa y a la red de la empresa.• Configurar estos dispositivos para forzar la introducción de contraseña.		2
<ul style="list-style-type: none">• Implementar mecanismos de filtrado de red, como firewalls y software de detección de intrusos.• Hacer cumplir las políticas adecuadas para controlar el tráfico entrante y saliente.		
<ul style="list-style-type: none">• Aplicar protocolos de seguridad aprobados a las conexiones de red.		
<ul style="list-style-type: none">• Configurar el equipo de red de forma segura.		
<ul style="list-style-type: none">• Encriptar la información en tránsito de acuerdo a su clasificación.		3
<ul style="list-style-type: none">• Establecer y mantener una política para la seguridad de la conectividad con base en las evaluaciones de riesgo y los requisitos del negocio.		
<ul style="list-style-type: none">• Establecer mecanismos confiables para apoyar la transmisión y recepción segura de la información.		4
<ul style="list-style-type: none">• Llevar a cabo pruebas de penetración periódicas para determinar la idoneidad de la protección de la red.		
<ul style="list-style-type: none">• Llevar a cabo pruebas periódicas a la seguridad del sistema para determinar la idoneidad de la protección del sistema.		



Gestionar los Servicios de Seguridad

Componente: Procesos

Práctica de Gestión	Métricas Modelo
DSS05.02 Gestionar la seguridad de la conectividad y de la red. Usar medidas de seguridad y procedimientos de gestión relacionados para proteger la información a través de todos los métodos de conectividad.	<ul style="list-style-type: none">• Número de brechas del firewall• Número de vulnerabilidades descubiertas• Porcentaje de tiempo que la red y los sistemas no están disponibles debido a incidentes de seguridad
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Cybermaturity Platform, 2018	AC.MI Manage Network Integrity & Segregation; CM.MN Monitor Networks; AC.CP Manage Communication Protections
HITRUST CSF versión 9, septiembre de 2017	01.04 Network Access Control
ISF, The Standard of Good Practice for Information Security 2016	PA2.3 Mobile Device Connectivity; NC1.1 Network Device Configuration
ISO/IEC 27002:2013/Cor.2:2015(E)	13.1 Network security management
National Institute of Standards and Technology Special Publication 800–53, Revisión 5 (Borrador), agosto de 2017	3.20 System and information integrity (SI–8)
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, Agosto de 2016	CSC 9: Limitation and Control of Network Ports, Protocols, and Services; CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches



Gestionar los Servicios de Seguridad

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS05.03 Gestionar la seguridad de endpoint. Garantizar que los dispositivos de punto final (Endpoint, término en inglés) (ej. ordenador portátil, ordenador de sobremesa, servidor y otros dispositivos móviles o de red o software) tengan una seguridad a un nivel igual o superior al de los requisitos de seguridad definidos para la información procesada, almacenada o transmitida.	<ul style="list-style-type: none">• Número de incidentes que involucran a dispositivos endpoint• Número de dispositivos no autorizados detectados en la red o en el entorno de usuario final• Porcentaje de personas que reciben formación de concienciación relacionada con el uso de dispositivos endpoint	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">• Configurar los sistemas operativos de forma segura.		2
<ul style="list-style-type: none">• Implementar mecanismos de bloqueo de dispositivos.		
<ul style="list-style-type: none">• Gestionar el acceso y control remotos (ej. dispositivos móviles, teletrabajo)		
<ul style="list-style-type: none">• Gestionar la configuración de red de forma segura.		
<ul style="list-style-type: none">• Implementar el filtrado de tráfico de red en dispositivos de punto final.		
<ul style="list-style-type: none">• Proteger la integridad del sistema.		
<ul style="list-style-type: none">• Proporcionar protección física a los dispositivos de punto final.		
<ul style="list-style-type: none">• Eliminar de forma segura los dispositivos Endpoint		
<ul style="list-style-type: none">• Gestionar el acceso malicioso a través del correo electrónico y los navegadores web. Por ejemplo, bloquear determinados sitios web y desactivar los clics a enlaces para los smartphones.		
<ul style="list-style-type: none">• Encriptar la información almacenada de acuerdo a su clasificación.		3



Gestionar los Servicios de Seguridad

Componente: Procesos

Práctica de Gestión	Métricas Modelo
DSS05.03 Gestionar la seguridad de endpoint. Garantizar que los dispositivos de punto final (Endpoint, término en inglés) (ej. ordenador portátil, ordenador de sobremesa, servidor y otros dispositivos móviles o de red o software) tengan una seguridad a un nivel igual o superior al de los requisitos de seguridad definidos para la información procesada, almacenada o transmitida.	<ul style="list-style-type: none">• Número de incidentes que involucran a dispositivos endpoint• Número de dispositivos no autorizados detectados en la red o en el entorno de usuario final• Porcentaje de personas que reciben formación de concienciación relacionada con el uso de dispositivos endpoint
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Cybermaturity Platform, 2018	IP.MM Apply Mobile Device Management; TP.MP Apply Media Protection; DP.DP Detect Mobile Code and Browser Protection
ISF, The Standard of Good Practice for Information Security 2016	PM1.3 Remote Working; PA2.1 Mobile Device Configuration; PA2.4 Employeeowned Devices; PA2.5 Portable Storage Devices; NC1.6 Remote Maintenance
National Institute of Standards and Technology Special Publication 800–53, Revisión 5 (Borrador), agosto de 2017	3.4 Assessment, authorization and monitoring (CA–8, CA–9); 3.19 System and communications protection (SC–10)
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, Agosto de 2016	CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers; CSC 7: Email and Web Browser Protections



Gestionar los Servicios de Seguridad

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS05.04: Gestionar la identidad del usuario y el acceso lógico. <ul style="list-style-type: none">Asegurarse de que todos los usuarios tienen derechos de acceso a la información de acuerdo con los requisitos del negocio.Coordinarse con las unidades del negocio que gestionan sus propios derechos de acceso en los procesos de negocio.	<ul style="list-style-type: none">Tiempo promedio entre el cambio y la actualización de cuentasNúmero de cuentas (vs. número de usuarios/personal autorizado)Número de incidentes relacionados con el acceso no autorizado a la Información	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">Mantener los derechos de acceso de los usuarios de acuerdo con la función del negocio, los requisitos del proceso y las políticas de seguridad.Alinear la gestión de identidades y derechos de acceso con los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad–de–tener y necesidad–de–conocer.		2
<ul style="list-style-type: none">Administrar oportunamente todos los cambios en los derechos de acceso (creación, modificación y eliminación), basándose únicamente en transacciones aprobadas y documentadas que hayan sido autorizadas por personas designadas por la dirección.		3
<ul style="list-style-type: none">Segregar, reducir al mínimo necesario y gestionar activamente cuentas de usuario privilegiadas.Asegurar la supervisión de todas las actividades en estas cuentas.		
<ul style="list-style-type: none">Identificar de forma unívoca y por roles funcionales todas las actividades de procesamiento de información.Coordinarse con las unidades de negocio para asegurarse de que todos los roles están definidos de manera consistente, incluidos los roles definidos por el propio negocio dentro de las aplicaciones de procesos del negocio.		
<ul style="list-style-type: none">Autenticar todo el acceso a activos de información de acuerdo con el rol del individuo o a las reglas del negocio.Coordinarse con las unidades de negocio que gestionan la autenticación dentro de las aplicaciones utilizadas en los procesos de negocio, con el fin de asegurar que los controles de autenticación hayan sido administrados adecuadamente.		
<ul style="list-style-type: none">Garantizar que todos los usuarios (internos, externos y temporales) y su actividad en los sistemas de TI (aplicación de negocio, infraestructura de TI, operaciones, desarrollo y mantenimiento de sistemas) se puedan identificar de manera unívoca.		



Gestionar los Servicios de Seguridad

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS05.04: Gestionar la identidad del usuario y el acceso lógico. <ul style="list-style-type: none">Asegurarse de que todos los usuarios tienen derechos de acceso a la información de acuerdo con los requisitos del negocio.Coordinarse con las unidades del negocio que gestionan sus propios derechos de acceso en los procesos de negocio.	<ul style="list-style-type: none">Tiempo promedio entre el cambio y la actualización de cuentasNúmero de cuentas (vs. número de usuarios/personal autorizado)Número de incidentes relacionados con el acceso no autorizado a la Información	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">Mantener un registro de auditoría del acceso a la información dependiendo de su sensibilidad y de los requisitos regulatorios.		4
<ul style="list-style-type: none">Llevar a cabo revisiones gerenciales periódicas de todas las cuentas y privilegios relacionados.		
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica	
HITRUST CSF versión 9, septiembre de 2017	10.03 Cryptographic Controls	
ISF, The Standard of Good Practice for Information Security 2016	PM1.1 Employment Life Cycle; SA1 Access Management	
ISO/IEC 27002:2013/Cor.2:2015(E)	7.3 Termination and change of employment; 9. Access control	
ITIL V3, 2011	Service Operation, 4.5 Access Management	
National Institute of Standards and Technology Special Publication 800–53, Revisión 5 (Borrador), agosto de 2017	3.1 Access control (AC–11, AC–12); 3.11 Media protection (MP–2, MP–4, MP–7); 3.13 Physical and environmental protection (PE–2, PE–3, PE–6)	
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, Agosto de 2016	CSC 1: Inventory of Authorized and Unauthorized Devices; CSC 2: Inventory of Authorized and Unauthorized Software; CSC 5: Controlled Use of Administrative Privileges; CSC 16: Account Monitoring and Control	



Gestionar los Servicios de Seguridad

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS05.05 Gestionar el acceso físico a los activos de I&T. <ul style="list-style-type: none">Definir e implantar procedimientos (incluyendo procedimientos de emergencia) para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas, de acuerdo con las necesidades del negocio.El acceso a las instalaciones, edificios y áreas debe estar justificado, autorizado, registrado y supervisado.Este requisito aplica a todas las personas que accedan a las instalaciones, incluyendo personal interno, personal temporal, clientes, proveedores, visitantes y cualquier otro tercero.	<ul style="list-style-type: none">Calificación promedio de las evaluaciones de seguridad físicaNúmero de incidentes relacionados con la seguridad de la información física	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">Registrar y monitorizar todos los puntos de entrada a las instalaciones de TI.Registrar a todos los visitantes al sitio, incluidos contratistas y proveedores.		2
<ul style="list-style-type: none">Asegurar que todo el personal muestra una identificación debidamente autorizada en todo momento.		
<ul style="list-style-type: none">Requerir a los visitantes que estén acompañados en todo momento durante su estancia en las instalaciones.		
<ul style="list-style-type: none">Restringir y monitorizar el acceso a instalaciones sensibles de TI, mediante el establecimiento de restricciones al perímetro, como vallas, paredes y dispositivos de seguridad en puertas interiores y exteriores.		
<ul style="list-style-type: none">Gestionar solicitudes para permitir el acceso debidamente autorizado a las instalaciones de cómputo.		3
<ul style="list-style-type: none">Garantizar que los perfiles de acceso permanezcan actualizados.Basar el acceso a las instalaciones de TI (sala de servidores, edificios, áreas o zonas) en el cargo y las responsabilidades.		
<ul style="list-style-type: none">Realizar formación sobre concienciación de la seguridad de la información física de forma regular.		



Gestionar los Servicios de Seguridad

Componente: Procesos

Práctica de Gestión	Métricas Modelo
DSS05.05 Gestionar el acceso físico a los activos de I&T. <ul style="list-style-type: none">Definir e implantar procedimientos (incluyendo procedimientos de emergencia) para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas, de acuerdo con las necesidades del negocio.El acceso a las instalaciones, edificios y áreas debe estar justificado, autorizado, registrado y supervisado.Este requisito aplica a todas las personas que accedan a las instalaciones, incluyendo personal interno, personal temporal, clientes, proveedores, visitantes y cualquier otro tercero.	<ul style="list-style-type: none">Calificación promedio de las evaluaciones de seguridad físicaNúmero de incidentes relacionados con la seguridad de la información física
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Cybermaturity Platform, 2018	AC.MA Manage Access; ID.DI Determine Impacts
HITRUST CSF versión 9, septiembre de 2017	01.01 Business Requirement for Access Control; 01.02 Authorized Access to Information Systems; 02.0 Human Resources Security
ISF, The Standard of Good Practice for Information Security 2016	NC1.2 Physical Network Management
ISO/IEC 27002:2013/Cor.2:2015(E)	11. Physical and environmental security



Gestionar los Servicios de Seguridad

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS05.06: Gestionar documentos sensibles y dispositivos de salida. Establecer protecciones físicas apropiadas, prácticas contables y gestión de inventario relativa a activos sensibles de I&T, como formas especiales, instrumentos negociables, impresoras para fines especiales o tokens de seguridad.	<ul style="list-style-type: none">• Número de dispositivos de salida robados.• Porcentaje de documentos sensibles y dispositivos de salida identificados en el inventario	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">• Establecer procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa.		2
<ul style="list-style-type: none">• Asegurar que se han establecido controles criptográficos para proteger información sensible almacenada electrónicamente.		
<ul style="list-style-type: none">• Asignar privilegios de acceso a documentos sensibles y dispositivos de salida con base en el principio de menor privilegio, manteniendo un equilibrio entre el riesgo y los requisitos del negocio.		3
<ul style="list-style-type: none">• Establecer un inventario de documentos sensibles y dispositivos de salida y realizar reconciliaciones periódicas.		
<ul style="list-style-type: none">• Establecer salvaguardas físicas adecuadas para documentos sensibles.		



Gestionar los Servicios de Seguridad

Componente: Procesos

Práctica de Gestión	Métricas Modelo
DSS05.06: Gestionar documentos sensibles y dispositivos de salida. Establecer protecciones físicas apropiadas, prácticas contables y gestión de inventario relativa a activos sensibles de I&T, como formas especiales, instrumentos negociables, impresoras para fines especiales o tokens de seguridad.	<ul style="list-style-type: none">Número de dispositivos de salida robados.Porcentaje de documentos sensibles y dispositivos de salida identificados en el inventario
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Cybermaturity Platform, 2018	CM.Ph Monitor Physical
HITRUST CSF versión 9, septiembre de 2017	01.06 Application & Information Access Control; 01.07 Mobile Computing & Teleworking; 08.0 Physical & Environmental Security; 10.03 Cryptographic Controls; 10.04 Security of System Files
ISF, The Standard of Good Practice for Information Security 2016	IR2.3 Business Impact Assessment – Confidentiality Requirements; IR2.4 Business Impact Assessment – Integrity Requirements; IR2.5 Business Impact Assessment – Availability Requirements; IM2.2 Sensitive Physical Information; PA2.2 Enterprise Mobility Man
ISO/IEC 27002:2013/Cor.2:2015(E)	10. Cryptography
National Institute of Standards and Technology Special Publication 800–53, Revisión 5 (Borrador), agosto de 2017	3.1 Access control (AC–2, AC–3, AC–4, AC–5, AC–6, AC–13, AC–24); 3.7 Identification and authentication (IA–2, IA–10, IA–11)
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, Agosto de 2016	CSC 15: Wireless Access Control



Gestionar los Servicios de Seguridad

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad. <ul style="list-style-type: none">Mediante el uso de un portafolio de herramientas y tecnologías (ej. herramientas de detección de intrusión), gestionar las vulnerabilidades y monitorizar la infraestructura para detectar accesos no autorizados.Asegurar que las herramientas, tecnologías y detección de seguridad están integradas en la monitorización general de eventos y la gestión de incidentes.	<ul style="list-style-type: none">Número de pruebas de vulnerabilidad llevadas a cabo en dispositivos perimetralesNúmero de vulnerabilidades descubiertas durante las pruebasTiempo dedicado a remediar vulnerabilidadesPorcentaje de tickets creados de forma oportuna cuando los sistemas de monitorización identifican posibles incidentes de seguridad.	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">Usar de forma continua un portafolio de tecnologías, servicios y activos soportados (ej. escáneres de vulnerabilidad, fuzzers y sniffers, analizadores de protocolos) para identificar vulnerabilidades de seguridad de la información.		2
<ul style="list-style-type: none">Definir y comunicar escenarios de riesgo para que se puedan reconocer con facilidad y se pueda entender su probabilidad e impacto.		
<ul style="list-style-type: none">Revisar regularmente los logs de eventos para detectar posibles incidentes.		
<ul style="list-style-type: none">Garantizar que se creen tickets relativos a incidentes de seguridad de forma oportuna cuando la monitorización identifique posibles incidentes.		
<ul style="list-style-type: none">Registrar eventos relacionados con la seguridad y conservar los registros durante el periodo de tiempo apropiado.		3
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
ISF, The Standard of Good Practice for Information Security 2016		IR2.6 Threat Profiling
National Institute of Standards and Technology Special Publication 800–53, Revisión 5 (Borrador), agosto de 2017		3.7 Identification and authentication (IA–3); 3.11 Media protection (MP–1); 3.13 Physical and environmental protection (PE–5); 3.19 System and communications protection (SC–15)
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, Agosto de 2016		Maintenance, Monitoring, and Analysis of Audit Logs



Gestionar los Servicios de Seguridad

Componentes: Estructuras Organizativas

	D i r e c t o r d e T I	D i r e c t o r d e s e g u r i d a d d e l a i n f o r m a c i ó n	D u e ñ o s d e l p r o c e s o d e n e g o c i o	D i r e c t o r d e R e c u r s o s H u m a n o s	J e f e d e d e s a r r o l l o	J e f e d e o p e r a c i o n e s d e T I	G e s t o r d e s e g u r i d a d d e l a i n f o r m a c i ó n	D i r e c t o r d e p r i v a c i d a d
Práctica clave de gestión								
DSS05.01 Proteger contra software malicioso		A	R	R	R	R	R	
DSS05.02 Gestionar la seguridad de la conectividad y de la red.		A			R	R	R	
DSS05.03 Gestionar la seguridad de endpoint.		A			R	R	R	
DSS05.04 Gestionar la identidad del usuario y el acceso lógico.		A	R			R	R	R



Gestionar los Servicios de Seguridad

Componentes: Flujos y elementos de información

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS05.01 Proteger contra software malicioso			Política de prevención de software malicioso	APO01.02
			Evaluaciones de amenazas potenciales	APO12.02; APO12.03
DSS05.02 Gestionar la seguridad de la conectividad y de la red.	APO01.07	Directrices de clasificación de datos	Política de seguridad de la conectividad	APO01.02
	APO09.03	SLAs	Resultados de pruebas de penetración	MEA04.07
DSS05.03 Gestionar la seguridad de endpoint.	APO03.02	Modelo de arquitectura de la información	Políticas de seguridad para dispositivos Endpoint	APO01.02
	APO09.03	<ul style="list-style-type: none">• SLAs• OLAs		
	BAI09.01	Resultados de comprobaciones de inventario físicas		
	DSS06.06	Informes de violaciones		



Gestionar los Servicios de Seguridad

Componentes: Flujos y elementos de información

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	APO01.05	Definición de roles y responsabilidades relacionadas con I&T	Resultados de revisiones de cuentas de usuarios y privilegios	Interna
	APO03.02	Modelo de arquitectura de la información	Derechos de acceso de usuario aprobados	Interna
DSS05.05 Gestionar el acceso físico a los activos de I&T.			Registros de acceso	Interna
			Solicitudes de acceso aprobadas	Interna
DSS05.06: Gestionar documentos sensibles y dispositivos de salida.	APO03.02	Modelo de arquitectura de la información	Privilegios de acceso	Interna
			Inventario de documentos y dispositivos sensibles	Interna
DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad.			Tickets relacionados con incidentes de seguridad	DSS02.02
			Características de los incidentes de seguridad	Interna
			Logs de eventos de seguridad	Interna
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)			Referencia específica	
Sin documentación relacionada para este componente.				



Gestionar los Servicios de Seguridad

Componentes: Personas, habilidades y competencias

Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Seguridad de la información	Skills Framework for the Information Age V6, 2015	SCTY
Gestión de seguridad de la información	e-Competence Framework (e-CF) – A common European Framework for ICT Professionals in all industry sectors – Part 1: Framework, 2016	E. Manage – E.8. Information Security Management
Pruebas de penetración	Skills Framework for the Information Age V6, 2015	PENT
Administración de seguridad	Skills Framework for the Information Age V6, 2015	SCAD



Gestionar los Servicios de Seguridad

Componentes: Políticas y procedimientos

Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Política de seguridad de la información	<ul style="list-style-type: none">Establecer directrices para proteger la información corporativa y los sistemas e infraestructura asociados.		



Gestionar los Servicios de Seguridad

Componentes: Cultura, ética y comportamiento

Elementos culturales clave	Documentación relacionada	Referencia específica
<ul style="list-style-type: none">• Crear una cultura de concienciación con respecto a la responsabilidad del usuario de mantener prácticas de seguridad y de privacidad.	(1) HITRUST CSF versión 9, septiembre de 2017; (2) ISF, The Standard of Good Practice for Information Security 2016	(1) 01.03 User Responsibilities; (2) PM2.1 Security Awareness Program



Gestionar los Servicios de Seguridad

Componentes: Servicios, infraestructura y aplicaciones

- Servicios de directorio.
- Sistemas de filtrado de correo electrónico.
- Sistema de gestión de acceso e identidad.
- Servicios de concienciación sobre seguridad.
- Herramientas de seguridad de la información y de gestión de eventos (SIEM).
- Servicios del centro de operaciones de seguridad (SOC).
- Servicios de evaluación de seguridad de terceros.
- Sistemas de filtrado de URL.



Gestionar los Servicios de Seguridad

Resumen de Procesos de Gestionar los Servicios de Seguridad

- DSS05.01 Proteger contra software malicioso.
- DSS05.02 Gestionar la seguridad de la conectividad y de la red.
- DSS05.03 Gestionar la seguridad de endpoint.
- DSS05.04: Gestionar la identidad del usuario y el acceso lógico.
- DSS05.05 Gestionar el acceso físico a los activos de I&T.
- DSS05.06: Gestionar documentos sensibles y dispositivos de salida.
- DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad.





Gestionar los Servicios de Seguridad

Algunos Conceptos Clave

- **Email Proxy**
- Es un tipo de servidor proxy que se utiliza específicamente para gestionar el tráfico de correo electrónico. Funciona como intermediario entre el servidor de correo electrónico del remitente y el servidor de correo electrónico del destinatario, filtrando y reenviando los correos electrónicos según sea necesario.
- Los Email Proxies pueden tener varias funciones y usos, incluyendo:
 - **Seguridad:** El Email Proxy puede filtrar los correos electrónicos para detectar y bloquear correos no deseados (spam), phishing y malware antes de que lleguen al servidor de correo del destinatario.
 - **Rendimiento:** Almacenamiento temporal de correos electrónicos para mejorar el rendimiento y la eficiencia del servidor de correo del destinatario.
 - **Control de acceso:** Limitar el acceso a ciertos correos electrónicos o dominios, proporcionando un control más granular sobre el tráfico de correo electrónico.
 - **Cifrado:** Proporcionar cifrado de extremo a extremo para los correos electrónicos, protegiendo la privacidad y la seguridad de los datos.
- En resumen, un Email Proxy es una herramienta útil para gestionar y proteger el tráfico de correo electrónico, proporcionando seguridad, rendimiento y control mejorados.





Gestionar los Servicios de Seguridad

Algunos Conceptos Clave

- **Web Proxy**
- Es un servidor que actúa como intermediario entre los usuarios de una red y el internet. Cuando un usuario hace una solicitud para acceder a un sitio web a través de un proxy web, la solicitud se envía primero al servidor proxy, que luego la reenvía al sitio web deseado. Una vez que el servidor web responde, la respuesta se envía de vuelta al servidor proxy, que la reenvía al usuario.
- Los proxies web tienen varios usos y beneficios, incluyendo:
 - **Anonimato:**, la dirección IP real del usuario se oculta, lo que puede ayudar a proteger la privacidad y el anonimato en línea.
 - **Filtrado de contenido:** Algunos proxies web pueden filtrar el contenido de los sitios web, bloqueando el acceso a sitios web específicos o categorías de sitios web, como redes sociales o sitios de juegos, con el fin de mejorar la seguridad o la productividad.
 - **Caché:** Los proxies web pueden almacenar en caché las páginas web solicitadas, lo que puede mejorar la velocidad de carga de los sitios web al reducir la cantidad de datos que se deben enviar desde el servidor web original.
 - **Control de acceso:** Los proxies web pueden utilizarse para controlar el acceso a sitios web específicos, restringiendo el acceso a determinados usuarios o grupos de usuarios.
- En resumen, un proxy web es una herramienta útil para mejorar la privacidad, la seguridad y la eficiencia al acceder a internet.





Gestionar los Servicios de Seguridad

Algunos Conceptos Clave

- **IAM – Identity Access Management**
- Gestión de Identidad y Acceso, es un marco de políticas, tecnologías y procesos que garantiza que las personas y sistemas adecuados tengan acceso a los recursos adecuados en el momento adecuado y durante el tiempo adecuado. IAM se centra en la gestión de la identidad de los usuarios y el control de su acceso a sistemas, aplicaciones y datos dentro de una organización.
- Los principales objetivos de IAM son:
 - **Autenticación:** Verificar la identidad de los usuarios para garantizar que solo las personas autorizadas tengan acceso a los recursos de la organización.
 - **Autorización:** Determinar los niveles de acceso de los usuarios autorizados a recursos específicos, basados en sus roles y responsabilidades.
 - **Administración de identidades:** Gestionar el ciclo de vida de las identidades de usuario, desde la creación hasta la eliminación, incluida la gestión de cambios de roles y privilegios.
 - **Auditoría y cumplimiento:** Registrar y monitorear el acceso a los recursos para cumplir con los requisitos de cumplimiento y mejorar la seguridad.
- IAM es fundamental para garantizar la seguridad de la información y la protección de los datos confidenciales de una organización al garantizar que solo las personas autorizadas tengan acceso a ellos.





Gestionar los Servicios de Seguridad

Algunos Conceptos Clave

- **Security Awareness**
- La "conciencia de seguridad" se refiere al conocimiento y comprensión que tienen las personas dentro de una organización sobre las amenazas de seguridad cibernética y las prácticas recomendadas para mitigar esos riesgos. Es un componente crucial de la estrategia de seguridad de una organización, ya que las acciones y decisiones de los empleados pueden tener un impacto significativo en la seguridad de la información.
- La conciencia de seguridad se logra a través de programas de concienciación y capacitación en seguridad cibernética, que educan a los empleados sobre temas como la identificación de correos electrónicos de phishing, la creación de contraseñas seguras, la protección de información confidencial y el uso seguro de dispositivos y redes.
- Al aumentar la conciencia de seguridad entre los empleados, las organizaciones pueden reducir el riesgo de incidentes de seguridad cibernética, como fugas de datos, malware y ataques de phishing, y crear una cultura de seguridad sólida en toda la organización.





Gestionar los Servicios de Seguridad

Algunos Conceptos Clave

- **SIEM – Security Information and Event Management**
- Gestión de la Información y Eventos de Seguridad, se refiere a un enfoque integral para gestionar la seguridad de la información y eventos en una organización. Un SIEM combina dos tecnologías principales:
 - **Gestión de la información de seguridad (SIM – Security Information Management):** Recopila, analiza y presenta datos de registros de eventos de seguridad de varios dispositivos de red y sistemas, como firewalls, servidores, aplicaciones, etc.
 - **Gestión de eventos de seguridad (SEM – Security Event Management):** Monitorea y correlaciona eventos de seguridad en tiempo real para identificar posibles amenazas y responder de manera proactiva.
- Al combinar la SIM y la SEM, un SIEM puede proporcionar a las organizaciones una visión completa de su postura de seguridad, ayudando a identificar y responder a incidentes de seguridad de manera más eficiente. Un SIEM puede ayudar a detectar intrusiones, identificar actividades maliciosas, cumplir con los requisitos de cumplimiento y mejorar la respuesta a incidentes de seguridad.





Gestionar los Servicios de Seguridad

Algunos Conceptos Clave

- **SOC – Security Operations Center**
- El Centro de Operaciones de Seguridad es una unidad dentro de una organización encargada de monitorear, detectar, analizar y responder a incidentes de seguridad cibernética de manera proactiva y reactiva.
- Las funciones principales de un SOC incluyen:
 - **Monitoreo de seguridad:** Supervisar continuamente la infraestructura de TI y los sistemas de la organización en busca de posibles amenazas y vulnerabilidades.
 - **Detección de amenazas:** Identificar y analizar actividades sospechosas que podrían indicar un ataque cibernético en curso o inminente.
 - **Respuesta a incidentes:** Tomar medidas inmediatas para contener y mitigar los incidentes de seguridad una vez que se hayan detectado, con el objetivo de minimizar el impacto y restaurar la normalidad lo antes posible.
 - **Análisis forense:** Realizar análisis forenses para determinar la causa raíz de los incidentes de seguridad y recopilar pruebas para acciones legales posteriores.
 - **Gestión de la información de seguridad:** Recopilar, analizar y compartir información sobre amenazas y vulnerabilidades con otras partes interesadas internas y externas.
- Un SOC es fundamental para la gestión efectiva de la seguridad cibernética de una organización, ya que ayuda a garantizar una respuesta rápida y eficiente a las amenazas, minimizando así el riesgo de pérdida de datos y daños a la reputación.





Gestionar los Servicios de Seguridad

Algunos Conceptos Clave

- **NOC – Network Operations Center**
- Un Centro de Operaciones de Red es una instalación desde la cual se supervisan, controlan y gestionan redes de telecomunicaciones, sistemas informáticos y servicios en tiempo real. El NOC es responsable de garantizar que la red y los servicios asociados estén disponibles, funcionando correctamente y respondan a las necesidades de los usuarios finales.
- Las funciones principales de un NOC incluyen:
 - **Monitorización de redes:** Supervisar el estado de la red, incluyendo el rendimiento, la disponibilidad y la integridad de los dispositivos de red y los enlaces de comunicación.
 - **Gestión de incidentes:** Identificar, registrar y gestionar incidentes que afecten a la red y los servicios, garantizando una resolución rápida y eficiente.
 - **Mantenimiento preventivo:** Realizar tareas de mantenimiento programadas para garantizar la estabilidad y el rendimiento óptimo de la red.
 - **Soporte técnico:** Proporcionar soporte técnico a los usuarios finales y a otros equipos de la organización para resolver problemas relacionados con la red y los servicios.
 - **Gestión de cambios:** Coordinar e implementar cambios en la red y los servicios de acuerdo con las políticas y procedimientos establecidos.
- En resumen, un NOC es un componente crítico en la gestión de redes de telecomunicaciones y sistemas informáticos, garantizando la disponibilidad y el rendimiento de los servicios de red para satisfacer las necesidades de los usuarios finales.





Universidad de Santiago de Chile
Facultad de Ingeniería
Departamento de Informática

Gestión y Gobernanza TI

**Gestionar los Controles de Procesos
de Negocio**



Gestionar los Controles de Procesos de Negocio

Introducción

- DSS06 – Gestionar los Controles de Procesos de Negocio.
- Pertenece al Dominio de Gestión Entregar, Dar Servicio y Soporte (DSS – Deliver, Service and Support).





Gestionar los Controles de Procesos de Negocio

Introducción

EDM01—Garantizar el establecimiento y el mantenimiento del marco de gobierno

EDM02—Asegurar la realización de beneficios

EDM03—Asegurar la optimización del riesgo

EDM04—Asegurar la optimización de los recursos

EDM05—Asegurar la transparencia de las partes interesadas

APO01—Gestionar el marco de gestión de TI

APO02—Gestionar la estrategia

APO03—Gestionar la arquitectura de la empresa

APO04—Gestionar la innovación

APO05—Gestionar el portafolio

APO06—Gestionar el presupuesto y los costes

APO07—Gestionar los recursos humanos

APO08—Gestionar las relaciones

APO09—Gestionar los acuerdos de servicio

APO10—Gestionar los proveedores

APO11—Gestionar la calidad

APO12—Gestionar el riesgo

APO13—Gestionar la seguridad

APO014—Gestionar los datos

BAI01—Gestionar los programas

BAI02—Gestionar la definición de requisitos

BAI03—Gestionar la identificación y construcción de soluciones

BAI04—Gestionar la disponibilidad y capacidad

BAI05—Gestionar los cambios organizativos

BAI06—Gestionar los cambios de TI

BAI07—Gestionar la aceptación y la transición de los cambios de TI

BAI08—Gestionar el conocimiento

BAI09—Gestionar los activos

BAI10—Gestionar la configuración

BAI11—Gestionar los proyectos

MEA01—Gestionar la monitorización del rendimiento y la conformidad

MEA02—Gestionar el sistema de control interno

MEA03—Gestionar el cumplimiento de los requisitos externos

MEA04—Gestionar el aseguramiento

DSS01—Gestionar las operaciones

DSS02—Gestionar las solicitudes e incidentes de servicio

DSS03—Gestionar los problemas

DSS04—Gestionar la continuidad

DSS05—Gestionar los servicios de seguridad

DSS06—Gestionar los controles de procesos de negocio

Entregar, Dar Servicio y Soporte (DSS – Deliver, Service and Support)



Gestionar los Controles de Procesos de Negocio

Descripción

- Definir y mantener los controles apropiados de los procesos de negocio para asegurar que la información relacionada y procesada por procesos de negocio internos o externalizados cumpla con todos los requisitos relevantes de control de la información.
- Identificar los requisitos relevantes de control de la información.
- Gestionar y operar los controles adecuados de entrada, throughput y salida (controles de aplicación) para asegurar que la información y el procesamiento de la información cumpla con estos requisitos.





Gestionar los Controles de Procesos de Negocio

Propósito

- Mantener la integridad de la información y la seguridad de los activos de información manejados dentro de los procesos de negocio, dentro de la empresa u operación externalizada.





Gestionar los Controles de Procesos de Negocio

Componentes


- Procesos (6):
 - DSS06.01 Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales.
 - DSS06.02: Controlar el procesamiento de información.
 - DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad.
 - DSS06.04 Gestionar errores y excepciones.
 - DSS06.05 Asegurar la trazabilidad y la rendición de cuentas de los eventos de información.
 - DSS06.06 Asegurar los activos de información.
- Estructuras organizativas.
- Flujos y elementos de información.
- Personas, habilidades y competencias (2).
- Políticas y procedimientos (1).
- Cultura, ética y comportamiento (1).
- Servicios, infraestructura y aplicaciones (2).





Gestionar los Controles de Procesos de Negocio


El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:

Metas Empresariales			Metas de Alineamiento	
<ul style="list-style-type: none">EG01 – Portafolio de productos y servicios competitivosEG05 – Cultura de servicio orientada al clienteEG08 – Optimización de la funcionalidad de procesos internos del negocioEG12 – Programas de transformación digital gestionados			<ul style="list-style-type: none">AG08 – Habilitar y dar soporte a procesos de negocio mediante la integración de aplicaciones y tecnología	
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento	
EG01	<ul style="list-style-type: none">Porcentaje de productos y servicios que cumplen o exceden los objetivos de ingresos y/o cuota de mercadoPorcentaje de productos y servicios que cumplen o exceden los objetivos de satisfacción del clientePorcentaje de productos y servicios que proporcionan una ventaja competitivaPlazo de comercialización para nuevos productos y servicios		AG08	<ul style="list-style-type: none">Plazo para la ejecución de servicios y procesos empresarialesNúmero de programas empresariales facilitados por I&T retrasados o que incurren en costes adicionales debido a problemas de integración tecnológicaNúmero de cambios en los procesos de negocio que se deben aplazar o revisar debido a problemas de integración tecnológicaNúmero de aplicaciones o infraestructuras críticas que operan en silos y no están integradas
EG05	<ul style="list-style-type: none">Número de interrupciones del servicio al clientePorcentaje de partes interesadas del negocio satisfechas de que la prestación de servicios al cliente cumpla con los niveles acordadosc. Número de quejas de clientesd. Tendencia de los resultados de la encuesta de satisfacción al cliente			



Gestionar los Controles de Procesos de Negocio

El objetivo de gestión respalda la consecución de una serie de metas empresariales y de alineamiento primordiales:

Metas Empresariales			Metas de Alineamiento	
<ul style="list-style-type: none">EG01 – Portafolio de productos y servicios competitivosEG05 – Cultura de servicio orientada al clienteEG08 – Optimización de la funcionalidad de procesos internos del negocioEG12 – Programas de transformación digital gestionados			<ul style="list-style-type: none">AG08 – Habilitar y dar soporte a procesos de negocio mediante la integración de aplicaciones y tecnología	
Métricas modelo para metas empresariales			Métricas modelo para metas de alineamiento	
EG08	<ul style="list-style-type: none">Niveles de satisfacción del consejo de administración y la dirección ejecutiva con las capacidades del proceso empresarialNiveles de satisfacción de los clientes con las capacidades de prestación de serviciosNiveles de satisfacción de los proveedores con las capacidades de la cadena de suministro		AG08	<ul style="list-style-type: none">Plazo para la ejecución de servicios y procesos empresarialesNúmero de programas empresariales facilitados por I&T retrasados o que incurren en costes adicionales debido a problemas de integración tecnológicaNúmero de cambios en los procesos de negocio que se deben aplazar o revisar debido a problemas de integración tecnológicaNúmero de aplicaciones o infraestructuras críticas que operan en silos y no están integradas
EG12	<ul style="list-style-type: none">Número de programas ejecutados a tiempo y dentro del presupuestoPorcentaje de partes interesadas satisfechas con la ejecución del programaPorcentaje de programas de transformación del negocio paradosPorcentaje de programas de transformación del negocio con actualizaciones regulares del estado reportado			



Gestionar los Controles de Procesos de Negocio

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS06.01 Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales. Evaluar y monitorizar continuamente la ejecución de las actividades de los procesos de negocio y los controles relacionados (basados en el riesgo empresarial) para asegurarse de que los controles de procesamiento están alineados con las necesidades del negocio.	<ul style="list-style-type: none">• Porcentaje de inventario de procesos críticos y controles clave completado• Porcentaje de controles de procesamiento alineados con las necesidades empresariales	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">• Identificar y documentar las actividades de control necesarias para procesos clave del negocio para satisfacer los requisitos de control para los objetivos estratégicos, operativos, de reporte y de cumplimiento.		2
<ul style="list-style-type: none">• Priorizar las actividades de control de acuerdo al riesgo inherente al negocio.• Identificar controles clave.		
<ul style="list-style-type: none">• Garantizar la propiedad de las actividades de control clave.		
<ul style="list-style-type: none">• Implementar controles automáticos.		3
<ul style="list-style-type: none">• Monitorizar continuamente las actividades de control de principio a fin para identificar oportunidades de mejora.		4
<ul style="list-style-type: none">• Mejorar de forma continua el diseño y operación de los controles de proceso del negocio.		5
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica
National Institute of Standards and Technology Special Publication 800–37, Revisión 2 (Borrador), mayo de 2018		3.1 Preparation (Task 10, 11)
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, Agosto de 2016		CSC 14: Controlled Access Based on the Need to Know



Gestionar los Controles de Procesos de Negocio

Componente: Procesos

Práctica de Gestión	Métricas Modelo
DSS06.02: Controlar el procesamiento de información. <ul style="list-style-type: none">Gestionar la ejecución de las actividades de los procesos del negocio y los controles relacionados, con base en el riesgo empresarial.Garantizar que el procesamiento de información sea válido, completo, preciso, oportuno y seguro (ej. refleja el uso legítimo y autorizado del negocio).	<ul style="list-style-type: none">Número de incidentes y hallazgos de auditoría que indican un fallo de los controles clavePorcentaje de cobertura de controles clave dentro de los planes de prueba
Actividades	Nivel de Capacidad
<ul style="list-style-type: none">Autenticar al originador de las transacciones y comprobar que el individuo tiene la autoridad para originar la transacción.Garantizar una adecuada segregación de tareas con relación al origen y aprobación de las transacciones.	2
<ul style="list-style-type: none">Comprobar que las transacciones son precisas, completas y válidas.Los controles podrían incluir secuencia, límite, rango, validez, razonabilidad, comprobación de tablas, existencia, verificación de clave, dígito de verificación, completitud, comprobaciones de duplicados y relaciones lógicas y ediciones temporales.Los criterios y parámetros de validación deberían estar sujetos a revisiones y confirmaciones periódicas.Validar los datos de entrada y editarlos o, cuando sea aplicable, devolverlos para su corrección lo más cerca posible del punto de origen.	3
<ul style="list-style-type: none">Sin comprometer los niveles de autorización de la transacción original, corregir y reenviar los datos que se introdujeron de forma errónea.Cuando sea adecuado para la reconstrucción, conservar documentos fuente originales durante el periodo de tiempo adecuado.	
<ul style="list-style-type: none">Mantener la integridad y la validez de los datos durante el ciclo de procesamiento.Asegurar que la detección de transacciones erróneas no interrumpe el procesamiento de transacciones válidas.	
<ul style="list-style-type: none">Manipular el resultado de forma autorizada, entregarlo al destinatario adecuado y proteger la información durante la transmisión.Verificar la exactitud e integridad del resultado.	



Gestionar los Controles de Procesos de Negocio

Componente: Procesos

Práctica de Gestión		Métricas Modelo	
DSS06.02: Controlar el procesamiento de información. <ul style="list-style-type: none">• Gestionar la ejecución de las actividades de los procesos del negocio y los controles relacionados, con base en el riesgo empresarial.• Garantizar que el procesamiento de información sea válido, completo, preciso, oportuno y seguro (ej. refleja el uso legítimo y autorizado del negocio).		<ul style="list-style-type: none">• Número de incidentes y hallazgos de auditoría que indican un fallo de los controles clave• Porcentaje de cobertura de controles clave dentro de los planes de prueba	
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">• Mantener la integridad de los datos durante interrupciones inesperadas en el procesamiento del negocio.• Confirmar la integridad de los datos después de fallos en el procesamiento.			3
<ul style="list-style-type: none">• Antes de pasar datos de transacciones entre aplicaciones internas y funciones operativas/de negocio (dentro o fuera de la empresa), comprobar el trato adecuado, la autenticidad del origen y la integridad del contenido.• Mantener la autenticidad y la integridad durante la transmisión o el transporte.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
HITRUST CSF versión 9, septiembre de 2017		13.01 Openness and Transparency; 13.02 Individual Choice and Participation	
ISF, The Standard of Good Practice for Information Security 2016		BA1.4 Information Validation	



Gestionar los Controles de Procesos de Negocio

Componente: Procesos

Práctica de Gestión	Métricas Modelo	
DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad. <ul style="list-style-type: none">Gestionar los roles de negocio, responsabilidades, niveles de autoridad y segregación de funciones necesarias para apoyar los objetivos de los procesos de negocio.Autorizar el acceso a todos los activos de información relacionados con los procesos de información del negocio, incluidos aquellos bajo custodia del negocio, de TI y de terceros.Esto asegura que la empresa sepa dónde están los datos y quién está manejando los datos en su nombre.	<ul style="list-style-type: none">Número de incidentes y hallazgos de auditoría debido a violaciones de acceso o de separación de funcionesPorcentaje de roles de procesos de negocio con derechos de acceso y niveles de autoridad asignadosPorcentaje de roles de proceso de negocio con clara separación de funciones	
Actividades		Nivel de Capacidad
<ul style="list-style-type: none">Asignar roles y responsabilidades conforme a las descripciones del cargo y las actividades aprobadas del proceso de negocio.		2
<ul style="list-style-type: none">Asignar niveles de autoridad para la aprobación de transacciones, límites de transacción y cualquier otra decisión relacionada con el proceso de negocio, conforme a roles de trabajo aprobados.		
<ul style="list-style-type: none">Asignar roles para actividades sensibles para que haya una clara segregación de funciones.		
<ul style="list-style-type: none">Asignar derechos de acceso y privilegios basado en lo mínimo requerido para realizar las actividades laborales, conforme a roles de trabajo predefinidos.Eliminar o revisar derechos de acceso de forma inmediata si el rol de trabajo cambia o si un miembro del personal deja el área de proceso de negocio.Revisar periódicamente para asegurar que el acceso sea adecuado para las amenazas, riesgo, tecnología y necesidades empresariales actuales.		3
<ul style="list-style-type: none">Concienciar y formar regularmente sobre los roles y responsabilidades, para que todos entiendan sus responsabilidades; la importancia de los controles; y la seguridad, integridad, confidencialidad y privacidad de la información de la compañía en todas sus formas.		
<ul style="list-style-type: none">Garantizar que los privilegios administrativos están asegurados, rastreados y controlados de forma suficiente y eficaz para prevenir el mal uso.		



Gestionar los Controles de Procesos de Negocio

Componente: Procesos

Práctica de Gestión		Métricas Modelo	
DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad. <ul style="list-style-type: none">Gestionar los roles de negocio, responsabilidades, niveles de autoridad y segregación de funciones necesarias para apoyar los objetivos de los procesos de negocio.Autorizar el acceso a todos los activos de información relacionados con los procesos de información del negocio, incluidos aquellos bajo custodia del negocio, de TI y de terceros.Esto asegura que la empresa sepa dónde están los datos y quién está manejando los datos en su nombre.		<ul style="list-style-type: none">Número de incidentes y hallazgos de auditoría debido a violaciones de acceso o de separación de funcionesPorcentaje de roles de procesos de negocio con derechos de acceso y niveles de autoridad asignadosPorcentaje de roles de proceso de negocio con clara separación de funciones	
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">Revisar periódicamente las definiciones de control de acceso, los logs y los informes de excepción.Asegurar que todos los privilegios de acceso son válidos y están alineados con los miembros actuales del personal y sus roles asignados.			4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
HITRUST CSF versión 9, septiembre de 2017		13.04 Collection, Use and Disclosure	
ISO/IEC 27002:2013/Cor.2:2015(E)		7. Human resource security	
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016		CSC 5: Controlled Use of Administrative Privileges	



Gestionar los Controles de Procesos de Negocio

Componente: Procesos

Práctica de Gestión		Métricas Modelo	
DSS06.04 Gestionar errores y excepciones. <ul style="list-style-type: none">Gestionar las excepciones y los errores del proceso del negocio y facilitar su corrección, mediante la ejecución de las acciones correctivas definidas y su escalamiento, si fuera necesario.Este tratamiento de excepciones y errores ofrece garantía de la precisión e integridad de los procesos de información del negocio.		<ul style="list-style-type: none">Frecuencia de las ineficiencias de procesamiento debido a entradas de datos incompletasNúmero de errores detectados a tiempoNúmero de errores de procesamiento de datos que se solucionaron de forma eficiente	
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">Revisar errores, excepciones y desviaciones.			2
<ul style="list-style-type: none">Hacer un seguimiento, corregir, aprobar y reenviar los documentos fuente y las transacciones.			
<ul style="list-style-type: none">Mantener evidencia de acciones correctivas.			
<ul style="list-style-type: none">Definir y mantener procedimientos para asignar la propiedad de errores y excepciones, corregir errores, anular errores y manejar condiciones fuera del balance.			3
<ul style="list-style-type: none">Informar de manera oportuna sobre errores relevantes de procesamiento de la información del negocio para realizar un análisis de causa raíz y de tendencia.			4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin documentación relacionada para esta práctica de gestión			



Gestionar los Controles de Procesos de Negocio

Componente: Procesos

Práctica de Gestión		Métricas Modelo	
DSS06.05 Asegurar la trazabilidad y la rendición de cuentas de los eventos de información. <ul style="list-style-type: none">Asegurarse de que la información de negocio puede rastrearse hasta el evento de negocio que la originó y se puede asociar a las partes que rinden cuentas.Esta capacidad de descubrimiento ofrece la garantía de que la información de negocio es confiable y que se ha tratado de acuerdo con los objetivos definidos.		<ul style="list-style-type: none">Número de incidentes en los que no se puede recuperar el historial de transaccionesPorcentaje de integridad del log de transacciones rastreables	
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">Obtener la información fuente, evidencias de soporte y el registro de transacciones.			2
<ul style="list-style-type: none">Definir los requisitos de retención de acuerdo a los requisitos del negocio para cumplir con las necesidades operativas, de reportes financieros y de cumplimiento.			3
<ul style="list-style-type: none">Disponer de la información fuente, las evidencias de soporte y el registro de las transacciones conforme a la política de retención.			
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
Sin documentación relacionada para esta práctica de gestión			



Gestionar los Controles de Procesos de Negocio

Componente: Procesos

Práctica de Gestión		Métricas Modelo	
<ul style="list-style-type: none">• DSS06.06 Asegurar los activos de información.• Asegurar los activos de información accesibles por el negocio a través de métodos aprobados, incluyendo información en formato electrónico (ej. dispositivos de medios portátiles, aplicaciones de usuarios y dispositivos de almacenamiento, u otros métodos que crean nuevos activos de cualquier tipo), información en formato físico (ej. documentos fuente o informes de salida) e información durante el tránsito.• Esto beneficia al negocio porque ofrece una protección de principio a fin de la información.		<ul style="list-style-type: none">• Casos de datos de transacciones sensibles enviados al destinatario erróneo• Frecuencia de integridad de datos críticos comprometida	
Actividades			Nivel de Capacidad
<ul style="list-style-type: none">• Restringir el uso, distribución y el acceso físico a la información de acuerdo con su clasificación.• Proporcionar una concienciación y formación adecuada sobre el uso.			2
<ul style="list-style-type: none">• Aplicar las políticas y procedimientos de seguridad para la clasificación y uso aceptable de datos y para proteger los activos de información que están bajo control del negocio.• Identificar e implantar procesos, herramientas y técnicas para verificar el cumplimiento de forma razonable.			3
<ul style="list-style-type: none">• Informar al negocio y a otras partes interesadas sobre violaciones y desviaciones.			4
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)		Referencia específica	
CMMI Cybermaturity Platform, 2018		AC.MP Manage Access Permissions	
The CIS Critical Security Controls for Effective Cyber Defense Versión 6.1, agosto de 2016		CSC 18: Application Software Security	



Gestionar los Controles de Procesos de Negocio

Componentes: Estructuras Organizativas

	C o m i t é E j e c u t i v o	D i r e c t o r d e T I	C o n s e j o d e g o b i e r n o d e I & T	D i r e c t o r d e s e g u r i d a d d e l a i n f o r m a c i ó n	D u e ñ o s d e l p r o c e s o d e n e g o c i o	F u n c i ó n d e g e s t i ó n d e d a t o s	G e s t i o n d e s e r v i c i o s	G e s t o r d e s e g u r i d a d d e l a i n f o r m a c i ó n	A s e s o r j u r í d i c o
Práctica clave de gestión									
DSS06.01 Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales.	R		A		R				
DSS06.02 Controlar el procesamiento de información.		R	A	R	R	R	R		R
DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad.		R	A	R	R			R	



Gestionar los Controles de Procesos de Negocio

Componentes: Flujos y elementos de información

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS06.01 Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales.	APO01.07	<ul style="list-style-type: none">• Directrices de clasificación de datos• Procedimientos de integridad de datos	Análisis de causa raíz y recomendaciones	BAI06.01; MEA02.04; MEA04.04; MEA04.06; MEA04.07
			Resultados de las revisiones de la efectividad del procesamiento	MEA02.04
DSS06.02: Controlar el procesamiento de información.	BAI05.05	Plan de operación y uso	Informes de control del procesamiento	Interna
	BAI07.02	Plan de migración		
DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad.	APO11.01	Roles, responsabilidades y derechos de decisión del sistema de gestión de la calidad (SGC)	Niveles de autoridad asignados	APO01.05
	APO13.01	Declaración del alcance del sistema de gestión de seguridad de la información (SGSI)	Roles y responsabilidades asignados	APO01.05
	DSS05.05	Logs de acceso	Derechos de acceso asignados	APO07.04
	EDM04.02	Responsabilidades asignadas para la gestión de recursos		



Gestionar los Controles de Procesos de Negocio

Componentes: Flujos y elementos de información

Práctica de gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
DSS06.04 Gestionar errores y excepciones.			Informes de error y análisis de causa raíz	Interna
			Evidencia de corrección y solución de errores	MEA02.04
DSS06.05 Asegurar la trazabilidad y la rendición de cuentas de los eventos de información.			Registro de transacciones	Interna
			Requisitos de retención	Interna; APO14.09
DSS06.06 Asegurar los activos de información.			Informes de violaciones	DSS05.03
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)			Referencia específica	
National Institute of Standards and Technology Special Publication 800–37, Revisión 2, septiembre de 2017			3.1 Preparation (Task 10, 11): Inputs and Outputs	



Gestionar los Controles de Procesos de Negocio

Componentes: Personas, habilidades y competencias

Habilidad	Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
Seguridad de la información	Skills Framework for the Information Age V6, 2015	SCTY
Administración de seguridad	Skills Framework for the Information Age V6, 2015	SCAD



Gestionar los Controles de Procesos de Negocio

Componentes: Políticas y procedimientos

Política relevante	Descripción de la política	Documentación relacionada	Referencia específica
Guía de los controles del negocio	<ul style="list-style-type: none">Define los controles del proceso de negocio para garantizar un control adecuado y reducir el riesgo de fraude y errores.Identifica controles manuales para proteger documentos (ej. fuente, entrada, procesamiento y documentos de salida); identifica los controles de supervisión para revisar el flujo de documentos y garantizar su correcto procesamiento.Incluye controles generales de I&T (ej. seguridad física, acceso y autenticación y gestión de cambios) y controles de aplicación (ej. comprobación de edición, configuración del sistema y ajustes de seguridad).		



Gestionar los Controles de Procesos de Negocio

Componentes: Cultura, ética y comportamiento

Elementos culturales clave	Documentación relacionada	Referencia específica
<ul style="list-style-type: none">• Crear una cultura que adopte la necesidad de controles sólidos en los procesos de negocio, mediante su incorporación en las aplicaciones en desarrollo o exigiéndolos en aplicaciones adquiridas o accedidas como un servicio.• Animar a todos los empleados a que sean conscientes de los controles para proteger todos los activos de la organización (ej. registros en papel e instalaciones)		



Gestionar los Controles de Procesos de Negocio

Componentes: Servicios, infraestructura y aplicaciones

- Controles automatizados de aplicación.
- Herramientas de auditoría de log de eventos.



Gestionar los Controles de Procesos de Negocio

Resumen de Procesos de Gestionar los Controles de Procesos de Negocio

- DSS06.01 Alinear las actividades de control incorporadas en los procesos de negocio con los objetivos empresariales.
- DSS06.02: Controlar el procesamiento de información.
- DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autoridad.
- DSS06.04 Gestionar errores y excepciones.
- DSS06.05 Asegurar la trazabilidad y la rendición de cuentas de los eventos de información.
- DSS06.06 Asegurar los activos de información.





Gestionar los Controles de Procesos de Negocio

Algunos Conceptos Clave

- **APM – Application Performance Management**
- La Gestión del Desempeño de Aplicaciones es una práctica o conjunto de herramientas y procesos utilizados para monitorear y gestionar el rendimiento y la disponibilidad de las aplicaciones informáticas en un entorno de producción.
- El objetivo principal es garantizar que las aplicaciones funcionen de manera eficiente y cumplan con los requisitos de rendimiento establecidos por la organización.
- El APM puede implicar el monitoreo de diversos aspectos de una aplicación, como la velocidad de respuesta, el tiempo de carga, el uso de recursos (como CPU y memoria), la capacidad de escala, entre otros.
- También puede incluir la identificación y resolución de cuellos de botella de rendimiento, la optimización del código y la mejora de la experiencia del usuario.
- En resumen, APM se enfoca en garantizar que las aplicaciones informáticas funcionen de manera óptima y brinden una experiencia satisfactoria al usuario final.





Universidad de Santiago de Chile
Facultad de Ingeniería
Departamento de Informática

Gestión y Gobernanza TI

Ejercicio



Ejercicio

Instrucciones

- Realizaremos 3 grupos.
- Según la visión y experiencia con Operaciones TI del DIINF que tienen los miembros del grupo:
 - Grupo 1:
 - ¿Operaciones TI tiene las condiciones para alcanzar el objetivo de gestión “Gestionar la continuidad” con un nivel de madurez 2?
 - Si no es así, mencione 3 actividades que crean las más importantes y justifique su grado de relevancia frente a las otras.
 - Grupo 2:
 - ¿Operaciones TI tiene las condiciones para alcanzar el objetivo de gestión “Gestionar los Servicios de Seguridad” con un nivel de madurez 2?
 - Si no es así, mencione 3 actividades que crean las más importantes y justifique su grado de relevancia frente a las otras.
 - Grupo 3:
 - ¿Operaciones TI tiene las condiciones para alcanzar el objetivo de gestión “Gestionar los Controles de Procesos de Negocio” con un nivel de madurez 2?
 - Si no es así, mencione 3 actividades que crean las más importantes y justifique su grado de relevancia frente a las otras.



Universidad de Santiago de Chile
Facultad de Ingeniería
Departamento de Informática

Gestión y Gobernanza TI

Resumen



Resumen

- El dominio de gestión “Entregar, Dar Servicio y Soporte” se encuentra es prácticamente operativo, pero de vital importancia para asegurar cada uno de los objetivos a través de cada una de las prácticas de gestión de ellos:
 - Gestionar las operaciones.
 - Gestionar las peticiones y los incidentes de servicio.
 - Gestionar los problemas.
 - Gestionar la continuidad.
 - Gestionar los servicios de seguridad.
 - Gestionar los controles de procesos de negocio.
- Las prácticas de gestión buscan que la misma nivele su madurez (al menos hasta nivel 2), y se pudieron ver muchas no se visualizan organizacionalmente, incluso en grandes organizaciones.
- Conseguir la madurez del nivel 2 puede significar un gran esfuerzo, y si a eso sumamos la aspiración a madurar más, pero lo mismo ayudará a conseguir las metas de alineamiento y, por ende, las metas de la empresa.





Universidad de Santiago de Chile
Facultad de Ingeniería
Departamento de Informática

Gestión y Gobernanza TI

Entregar, Dar Servicio y Soporte

Luis Berríos P.
1er Semestre 2025