

CODIGO	PROCESO	EDICIÓN	FECHA APROBACIÓN	PROPIETARIO
IMEE-10	GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	01.01	01/12/2014	IMEE
Descripción de Cambios sobre edición anterior		Proceso operativo definido en el Mapa de Procesos del IMEE. Revisión procesos		
Misión	El objetivo de la Gestión de la Seguridad de la información es cumplir con los requisitos de Seguridad acordados en los SLA y proveer un nivel de Seguridad básico.			
Alcance	Empieza: Se definen los requisitos y niveles de seguridad, estos requisitos se recogen en los SLA. Incluye: Planificación de los requisitos de seguridad, implementación de los planes, evaluación de la implementación y la infraestructura actual. Mantenimiento (mejoras basadas en lo aprendido, las evaluaciones y las regulaciones). Termina: Los informes se entregan a la gestión de niveles de servicio para que se informe al cliente del cumplimiento de la gestión de seguridad del acuerdo.			
ENTRADAS	ACTIVIDADES/TAREAS	SALIDAS	REVISADO/APROBADO POR	
<ul style="list-style-type: none"> - Política de Seguridad de la UPO. - Requisitos de seguridad de la información. - Acuerdos seguridad en SLAs. - Incidente severo en seguridad. - Revisión del Plan de Seguridad. - Análisis de riesgos y plan de continuidad. - Activos en CMDB. 	<ul style="list-style-type: none"> - Alcance, política y enfoque. - Evaluación de Riesgos. - Selección de objetivos de control. - Declaración de Riesgos. - Plan de tratamiento de riesgos. - Gestionar recursos de seguridad. - Gestionar incidentes severo. 	<ul style="list-style-type: none"> - Política de seguridad. - Evaluación de riesgos. - Plan de tratamiento de riesgos. - Declaración de riesgos. - Objetivos de control. - Controles y registros de seguridad. - Auditorías de seguridad. - Informes de seguridad. 	- Comisión de Garantía Interna de Calidad de IMEE.	
INFRAESTRUCTURAS	RECURSOS HUMANOS	DOCUMENTOS/NORMATIVA	REGISTROS	
<ul style="list-style-type: none"> - Espacios habilitados en IMEE. - Catalogo Servicios de IMEE. - Implementación pruebas, implantación. 	<ul style="list-style-type: none"> - Director de IMEE. - Responsable de Gestión de Proyectos y Servicios y Responsable de - Responsables servicios IMEE. - Responsable de Seguridad de la Información. 	<ul style="list-style-type: none"> - SLAs. - Normativas relativas a la seguridad de la información (Ley de protección de datos, norma 17799:2005 ...) - Documento de Prestación de servicios - Política de Seguridad de la UPO. 	<ul style="list-style-type: none"> - SLA - OLA - SLR - Contratos con terceros. - CMDB 	
INDICADORES	FORMULAS DE CALCULO	VARIABLES DE CONTROL	RESPONSABLE	
- Los indicados en el Cuadro de Mando Integral (CMI) de IMEE.	- Los indicados en el Cuadro de Mando Integral (CMI) de IMEE.	<ul style="list-style-type: none"> - Incidentes severo de seguridad - Acuerdos de confidencialidad. - SLR - SLA 	fceragu@admon.upo.es	

SEGURIDAD DE LA INFORMACIÓN

Dirección IMEE-UPO	Jefes de Gestión y Técnicos de IMEE	CGIC/Responsable	Procesos relacionados	DB/Doc. Referencia	Información Complementaria/Observaciones	Registros
					1) La Dirección de IMEE (Director, jefe de Gestión de Proyectos y servicios, Responsable de Planificación y Relaciones con los suministradores) junto con la Dirección de la UPO (Vicerrectorado con competencias de seguridad de la información, Gerencia, Comisión de Seguridad de la Información y Protección de Datos), definirán las políticas de seguridad de la Información en el ámbito de las infraestructuras de la UPO. La política es aprobada por los órganos de dirección de la UPO. https://upo.gob.es/opencms/AlfrescoFileTransferServlet?action=download&ref=6da8520d-ead4-11e2-9e20-e93b4c0e5b88	- Política de seguridad de la información..
					2) Definir los requisitos de seguridad de la información en base a los SLAs de los servicios de IMEE.	-SLA
					3) En esta fase se planifica la seguridad de la información en base a acuerdos de nivel de servicios, contratos de soporte, acuerdo de nivel de operaciones, políticas internas.	- Plan de seguridad de la información de IMEE.
					4) Se procede a la realización del análisis de riesgos. El análisis de riesgos se realizará con PILAR, conforme a los requerimientos exigidos en el ENS y conforma a norma ISO 27001. - Sistemas de información. - Servicios. - Aplicaciones y Software. - Infraestructuras. - Personas.	- Análisis de Riesgos -BD PILAR
MEJORAS A IMPLEMENTAR					5) Esta fase se inicia la implementación de los controles de seguridad (mejora la concienciación, clasificación y gestión de recursos, seguridad de personal, seguridad física, seguridad de infraestructuras, control de acceso a IMEE, gestión de los incidentes).	- Registros en PILAR.
MEJORAS A IMPLEMENTAR					6) Fase en la que se evalúa los controles de seguridad implementado (autoevaluación auditorías internas, auditorías externas).	- Informes seguimiento. - N/C
					7) Mantenimiento del Sistemas de Seguridad de la Información. Seguimiento de las incidencias y problemas de seguridad de la información.	- Incidentes - Problemas.