Anexo 2: Selección de Controles / Salvaguardas

Salvaguardas	Aspecto	Tipo de Protección	Madurez
Organización	PR	PTG	L0
Comité de gestión de seguridad de la información	PR	PTG	L0
Coordinación de la seguridad de la información	PR	PTG	L2
Asignación de responsabilidades para la seguridad de la información	PR	PTG	L3
Roles identificados	PR	PTG	L0
Política de Seguridad (documento)	PR	PTG	L0
Procedimiento derivado de la Política de Seguridad Global de la Organización	PR	PTG	L0
Está aprobado y respaldado por el responsable de la organización	PR	PTG	L0
Todo el personal de la organización tiene acceso al documento	PR	PTG	L0
Conocido y aceptado por los afectados	PR	PTG	L0
Referencia normativa y procedimientos específicos	PR	PTG	L0
Revisión periódica del documento de política	PR	PTG	L0
Documentación de seguridad del sistema	PR	PTG	L0
Procedimientos operativos	PR	PTG	L2
Criterios de aceptación para versiones o sistemas nuevos	PR	PTG	L1
Identificación y autenticación	PR	PTG	L2
Identificación de usuario	PR	PTG	L3
Herramientas de Identificación y Autenticación de usuario	PR	PTG	L2
Control de acceso lógico	PR	PTG	L0
Norma para el control de accesos	PR	PTG	L0
Restricción de acceso a la información	PR	PTG	L2
Segregación de tareas	PR	PTG	L1
Registro de usuario	PR	PTG	L3
Gestión de privilegios	PR	PTG	L3
Revisión de los derechos de acceso de los usuarios	PR	PTG	L1

Control de acceso discrecional	PR	PTG	L1
Control de acceso obligatorio	PR	PTG	L0
Uso de las utilidades del sistema	SW	PTG	L1
Conexión en terminales (logon)	SW	PTG	L1
Identificación automática de terminales	SW	PTG	L1
Limitación del tiempo de conexión	SW	PTG	L0
Desconexión automática de terminales	SW	PTG	L0
Gestión de incidencias	PR	PTG	L0
Procedimientos de gestión de incidentes	PR	PTG	L2
Frente a código dañino	SW	PTG	L2
Comunicación de las incidencias de seguridad	PR	PTG	L0
Comunicación de las deficiencias de seguridad	PR	PTG	L0
Comunicación de los fallos del software	SW	PTG	L0
Registro de fallos y revisión de las medidas correctoras	SW	PTG	L0
Se aprende de los incidentes y se proponen mejoras	PR	PTG	L2
Revisión de la seguridad de los sistemas de información	PR	PTG	L0
Continuidad del negocio (contingencia)	PR	PTG	L0
Proceso de gestión de la continuidad	PR	PTG	L0
Plan de gestión de crisis	PR	PTG	L0
Seguros contra interrupciones en el negocio	PR	PTG	L0
Registro y auditoría	PR	PTG	L2

Relaciones con terceros

Seguridad en los accesos de terceras partes	PR	PDI	L1
Establecimiento de acuerdos para intercambio de información y software	PR	PDI	L2
Inclusión de cláusulas de confidencialidad en los contratos con otras empresas	PR	PDI	L3

Instalaciones

Inventario de instalaciones	SF	PSF	L0
Normativa	PR	PSF	L1
Procedimientos	PR	PSF	L2

Diseño	PR	PSF	L3
Control de los accesos físicos	SF	PSF	L3
Protección del perímetro	SF	PSF	L3
Vigilancia	SF	PSF	L3
Iluminación de seguridad	SF	PSF	L3
Protección frente a desastres	SF	PSF	L2

Equipos informáticos (HW)

Inventario de equipos	HW	PHW	L1
Disponibilidad	HW	PHW	L0
Adquisición de HW	HW	PHW	L2
Instalación	HW	PHW	L2
Aplicación de perfiles de seguridad	HW	PHW	L0
Proceso de autorización de recursos para el tratamiento de la información	PR	PHW	L2
Protección física de los equipos	HW	PHW	L2
Equipo informático de usuario desatendido	HW	PHW	L0
Seguridad del equipamiento de oficina	HW	PHW	L2
Seguridad de los equipos fuera de las instalaciones	PR	PHW	L0
Protección de los dispositivos de red	HW	PHW	L2
Reproducción de documentos	PR	PTG	L2
Cambios (actualizaciones y mantenimiento)	PR	PTG	L0
Terminación	PR	PTG	L0

Aplicaciones (SW)

Inventario de aplicaciones	SW	PSW	L2
Copias de seguridad	SW	PSW	L2
Adquisición	SW	PSW	L2
Desarrollo	SW	PSW	L2
Puesta en producción	SW	PSW	L1
Aplicación de perfiles de seguridad	SW	PSW	L0
Explotación	SW	PSW	L2

Procedimiento para el control de software en producción	SW	PSW	L2
Seguridad de las aplicaciones	SW	PSW	L0
Seguridad de los ficheros del sistema	SW	PTG	L0
Seguridad de los ficheros de datos de la aplicación	SW	PTG	L2
Seguridad de los ficheros de configuración	SW	PTG	L2
Seguridad de los mecanismos de comunicación entre procesos	SW	PTG	L2
Procedimiento para detección de vulnerabilidades, y reacción ante las mismas	PR	PTG	L2
Cambios (actualizaciones y mantenimiento)	PR	PTG	L0
Seguimiento permanente de actualizaciones y parches	PR	PTG	L3
Evaluacion del impacto potencial del cambio	PR	PTG	L2
Definición del proceso de cambio de forma que minimice la interrupción del servicio	PR	PTG	L3
Retención de versiones anteriores de software como medida de precaución para contingencias	PR	PTG	L3
Pruebas de regresión	PR	PTG	L3
Procedimientos de control de cambios	PR	PTG	L3
Registro de toda actualización de SW	PR	PTG	L3
Documentación	PR	PTG	L3
Control de versiones de toda actualización del software	SW	PTG	L2
Actualización de todos los procedimientos de explotación afectados	PR	PTG	L3
Actualización de los planes de contingencia	PR	PTG	L0
Terminación	PR	PTG	L2
Norma para la eliminación de software	PR	PTG	L2

Datos / Información

Inventario de activos de información	PR	PDI	L0
Clasificación de la información	PR	PDI	L0
Disponibilidad	PR	PDI	L1
Integridad	PR	PDI	L1
Criptografía	PR	PDI	L1

Red

Inventario de servicios de comunicación	HW	PdC	L0

Disponibilidad	PR	PdC	L0
Adquisición o contratación	HW	PdC	L0
Planificación	HW	PdC	L0
Aceptación de nuevos servicios	HW	PdC	L1
Instalación	PR	PdC	L0
Aplicación de perfiles de seguridad	PR	PdC	L0
Operación	PR	PdC	L0
Control de acceso a la red	PR	PdC	L0
Acceso remoto	PR	PdC	L2
Norma de uso de los servicios de red	PR	PdC	L0
Autenticación de nodos de la red	PR	PdC	L1
Control del encaminamiento	PR	PdC	L0
Criptografía	PR	PdC	L3
Seguridad de los servicios de red	PR	PdC	L0
Protección de las comunicaciones Internet	PR	PdC	L2
Red privada virtual (VPN)	PR	PdC	L2
Protección emanaciones electromagnéticas	HW	PdC	L2
Cambios (actualizaciones y mantenimiento)	PR	PdC	L0
Seguimiento permanente de actualizaciones	PR	PdC	L1
Evaluación del impacto potencial del cambio	PR	PdC	L0
Definición del proceso de cambio de forma que minimice la interrupción del servicio	PR	PdC	L1
Pruebas de regresión	PR	PdC	L0
Procedimientos de control de cambios	PR	PdC	L0
Registro de toda actuación	PR	PdC	L0
Documentación	PR	PdC	L0
Actualización de todos los procedimientos de operación afectados	PR	PdC	L1
Actualización de los planes de contingencia	PR	PdC	L0
Terminación	PR	PdC	L0

Servicios

Inventario de servicios	PS	PdS	L0

Disponibilidad	PS	PDI	L0
Protección frente a DoS	PS	PdS	L0
Desarrollo	PS	PdS	L2
Despliegue	PS	PdS	L2
Procedimiento de puesta en pre-producción	PS	PDI	L2
Pruebas de aceptación	PS	PDI	L2
Procedimiento de paso a producción	PS	PDI	L2
Campaña de ejecución de pruebas de regresión (no afecta a los demás servicios)	PS	PDI	L2
Aplicación de perfiles de seguridad	PS	PDI	L1
Explotación	PS	PdS	L2
Norma de condiciones de uso	PS	PdS	L2
No repudio	PS	PdS	L3
Seguridad en comercio electrónico	PS	PdS	L3
Seguridad del correo electrónico	PS	PdS	L3
Protección de la integridad de la información publicada electrónicamente	PS	PdS	L2
Infraestructura de clave pública	PS	PdS	L2
Protección del directorio	PS	PdS	L2
Telefonía móvil	PS	PdS	L0
Teletrabajo	PS	PdS	L0
Gestión de servicios externos	PS	PdS	L3

Equipamiento Auxiliar

Inventario de equipamiento auxiliar	HW	PHW	L0
Disponibilidad	HW	PHW	L0
Instalaciones	HW	PHW	L0
Suministro eléctrico	HW	PHW	L3
Climatización	HW	PHW	L3
Protección del cableado	HW	PHW	L3
Otros suministros	HW	PHW	L2

Soportes de información

Inventario de soportes	HW	PHW	L3
Disponibilidad	HW	PHW	L3
Adquisición de soportes	HW	PHW	L3
Gestión de soportes	PR	PHW	L2
Herramientas para destrucción segura de información en soportes	HW	PHW	L1

Personal

Relación de personal	PP	PRP	L3
Puestos de trabajo	PP	PRP	L3
Contratación	PP	PRP	L3
Formación	PP	PRP	L3
Política del puesto de trabajo despejado y bloqueo de pantalla	PP	PRP	L3
Protección del usuario frente a coacciones	PP	PRP	L3