Seguridad 365

Elaboración SGSI Seguridad365 (Estado de cumplimiento)

Programa:	MISTIC
Empresa:	Seguridad365
Prueba:	TFM (Memoria)
Fecha:	21 de diciembre de 2018
Alumno:	José Alberto Catalá Hernansáiz
Universidad:	Universidad Oberta de Cataluña
Consultor:	Antonio José Segovia Henares

UOC Universitat Oberta de Catalunya

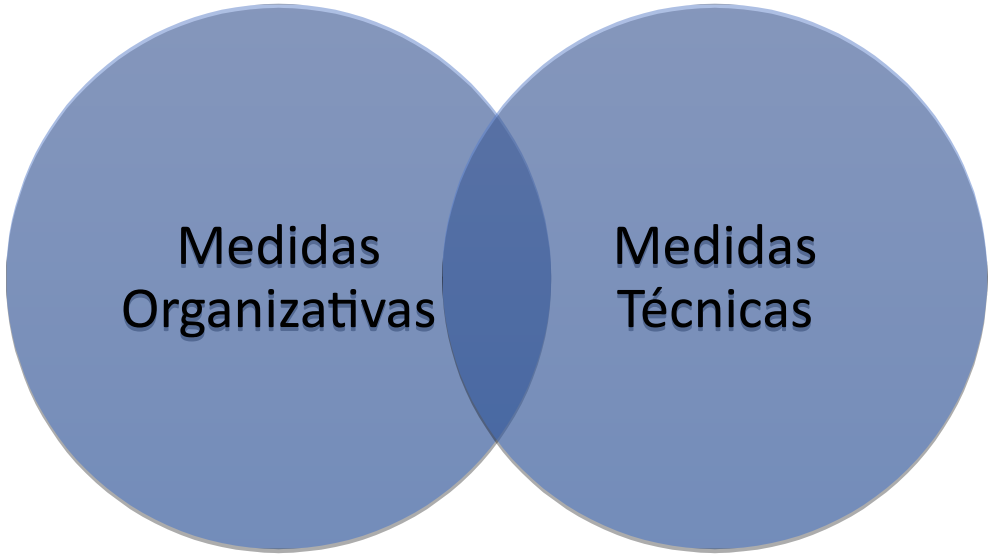
UAB Universitat Autònoma de Barcelona

UNIVERSITAT ROVIRA i VIRGILI

UIB Universitat de les Illes Balears

Propuestas de Mejora

Tipos de medidas de mejora



Mejoras Organizativas

Código: **MO-1**	*Proyecto:* **Plan de formación y concienciación a empleados**	
Presupuesto: N/A - Recursos propios	*Inicio: 3/12/2018*	*Fin: 1/2/2019*
Apartado Normativo 4. Contexto de la Organización 5. Liderazgo 7. Soporte *Controles* Políticas de Seguridad (5.1)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Elaborar un plan formativo y de capacitación de los empleados para el tratamiento adecuado de los sistemas de información. Incluye una campaña de concienciación del tratamiento de los datos de compañía y en particular de los datos de carácter personal.		
Objetivos: Incorporar acciones formativas genéricas al plan de formación de la compañía. Contratar cursos específicos para personal técnico y/o de compliance (sistemas de Gestión) Elaborar y difundir boletines periódicos de seguridad, buscando el impacto inmediato		
Responsable: • Director de RRHH	*Miembros implicados:* • CEO • CISO • Responsable de formación	

Mejoras Organizativas

Código: **MO-2**	*Proyecto:* **Implantación de sistema de gestión de usuarios y permisos**	
Presupuesto: N/A - Recursos propios	*Inicio: 3/12/2018*	*Fin: 14/2/2019*
Apartado Normativo 4. Contexto de la Organización 7. Soporte *Controles* Aspectos organizativos de la seguridad de la información (6.1) Control de accesos (9.4)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Análisis diseño y desarrollo de un sistema de gestión de usuarios, permisos y roles.		
Objetivos: Gestionar de forma adecuada el ciclo de vida de los usuarios, así como los permisos y roles otorgados a cada uno. Tener trazabilidad de los cambios de permiso de los usuarios. Verificar con la colaboración del Área de Formación, que un usuario tiene la formación necesaria para contar con determinados permisos.		
Responsable: • Director de RRHH	*Miembros implicados:* • CEO • CISO • Responsable de formación • CIO	

Mejoras Organizativas

Código: **MO-3**	*Proyecto:* **Política de gestión de incidentes de seguridad**	
Presupuesto: N/A - Recursos propios	*Inicio: 3/12/2018*	*Fin: 28/12/2018*
Apartado Normativo 4. Contexto de la Organización 7. Soporte *Controles* Políticas de Seguridad (5.1) Gestión de incidentes de seguridad de la información (16.1)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Hasta el momento no se gestionan de manera adecuada los incidentes de seguridad. Se les da tratamiento, peor no se informa a las autoridades competentes.		
Objetivos: Tener una política clara en cuanto al tratamiento de posibles incidentes de seguridad.		
Responsable: • CISO	*Miembros implicados:* • CEO • CIO	

Mejoras Organizativas

Código: **MO-4**	*Proyecto:* **Normativa de uso de dispositivos móviles y portátiles**	
Presupuesto: N/A - Recursos propios	*Inicio: 17/12/2018*	*Fin: 11/1/2019*
Apartado Normativo 4. Contexto de la Organización 7. Soporte *Controles* Políticas de Seguridad (5.1) Aspectos organizativos de la seguridad de la información (6.2)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Desarrollar una política de uso de dispositivos móviles y equipos portátiles. Hasta el momento no se hace firmar ningún documento a los empleados cuando reciben un dispositivo móvil o equipo portátil.		
Objetivos: Crear conciencia de uso adecuado de los dispositivos con los que la compañía dota a sus empleados. Por tanto, se espera que los empleados hagan un uso más adecuado y por tanto se eleve el umbral de seguridad en lo que a uso adecuado de dispositivo se refiere. Este proyecto se complementa con el plan formativo que se desarrolla en el proyecto MO-1.		
Responsable: • Director de RRHH	*Miembros implicados:* • CEO • CISO • Responsable de formación • CIO	

Mejoras Organizativas

Código: **MO-5**	*Proyecto:* **Acuerdos de confidencialidad con empleados**	
Presupuesto: N/A - Recursos propios	*Inicio: 28/12/2018*	*Fin: 25/1/2019*
Apartado Normativo 4. Contexto de la Organización 7. Soporte *Controles* Políticas de Seguridad (5.1) Seguridad Ligada a los Recursos Humanos (7.2, 7.3)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Desarrollo de una política de acuerdo de confidencialidad con respeto al empelado. Hasta el momento los empleados no firman ningún documento que les vincule con la obligación de preservar la información de compañía.		
Objetivos: Disponer de una política que firmará el empleado en su contratación y que tendrán que firmar los actuales empleados. Se espera disminuir el nivel de riesgo por uso inadecuado de la información. También está muy vinculado al plan formativo que se realizará en el proyecto MO-1.		
Responsable: • Director de RRHH	*Miembros implicados:* • CEO • CISO • Responsable de formación • CIO	

Mejoras Organizativas

Código: **MO-6**	*Proyecto:* **Acuerdos de confidencialidad con proveedores**	
Presupuesto: N/A - Recursos propios	*Inicio: 14/1/2019*	*Fin: 11/2/2019*
Apartado Normativo 5. Liderazgo *Controles* Políticas de Seguridad (5.1) Relación con suministradores (15.1)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Desarrollo de una política de acuerdo de confidencialidad con respeto a los proveedores. Si bien hasta el momento se viene firmando un acuerdo de confidencialidad (NDA), se considera necesario hacer una revisión de este.		
Objetivos: Crear un marco de trabajo con respecto a los proveedores que manejan información de la compañía, que proteja a Seguridad365 de eventuales incidentes de seguridad derivados del uso inadecuado por parte de proveedores.		
Responsable: • Director Asesoría Jurídica	*Miembros implicados:* • CEO • CISO • CFO • Responsable de Compras y Logística	

Mejoras Técnicas

Código: **MT-1**	*Proyecto:* **Instalación de consola centralizada antimalware**	
Presupuesto: 7.000 Euros 15% mantenimiento anual sobre esta cantidad	*Inicio: 3/21/2018*	*Fin: 28/12/2018*
Controles Seguridad en la operativa (12.2)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Si bien la compañía cuenta con antivirus instalado en servidores y PCs, no cuenta con una consola centralizada que controle el estado del antivirus en cada equipo. De manera que podría estar desactualizado o desinstalado eventualmente.		
Objetivos: Tener mayor control del estado del antivirus y de esta manera evitar posibles problemas con equipos desactualizados o incumpliendo la política de antivirus de la compañía.		
Responsable: • CIO	*Miembros implicados:* • CEO • CISO • CFO	

Mejoras Técnicas

Código: **MT-2**	*Proyecto:* **Implantación de gestor de dispositivos móviles (MDM)**	
Presupuesto: 3.000 Euros (Puesta en marcha) 25 euros por dispositivo anuales.	*Inicio: 10/12/2018*	*Fin: 3/5/2019*
Controles Aspectos normativos de la seguridad de la información (6.2) Gestión de activos (8.1)	*Activos afectados:* • Guardian365 • Exchange/SharePoint	
Descripción: La compañía entrega dispositivos móviles a sus empleados, pero no tiene control alguno sobre el dispositivo una vez entregado. Se afronta la instalación de un gestor de dispositivos móviles (MDM) que permita la administración de estos dispositivos de forma remota.		
Objetivos: Contar con una herramienta que permita aplicar políticas, desplegar aplicaciones, incluso formatear los dispositivos en caso de pérdida o robo.		
Responsable: • CIO	*Miembros implicados:* • CEO • CISO • CFO	

Mejoras Técnicas

Código: **MT-3**	*Proyecto:* **Cifrado de dispositivos móviles y portátiles**	
Presupuesto: N/A - Recursos propios	*Inicio: 7/1/2019*	*Fin: 8/3/2019*
Controles Aspectos normativos de la seguridad de la información (6.2) Cifrado (10.1)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Hasta el momento no hay una política clara de cifrado de dispositivos móviles y portátiles. De esta manera, nos podemos encontrar con equipos portátiles cifrados a voluntad del usuario. En este momento se quiere forzar por directivas el cifrado del dispositivo.		
Objetivos: Conseguir que todo el parque de dispositivos móviles y equipos portátiles estén cifrados.		
Responsable: • CIO	*Miembros implicados:* • CEO • CISO • CFO	

Mejoras Técnicas

Código: **MT-4**	*Proyecto:* **Implantación de Monitor de Red**	
Presupuesto: 17.000 Euros 20% mantenimiento anual sobre esta cantidad	*Inicio: 17/12/2018*	*Fin: 4/2/2019*
Controles Seguridad en las Telecomunicaciones (13.1)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Instalación y configuración de una herramienta que permita a los administradores de sistemas monitorizar la red en busca de posibles comportamientos anómalos que pudieran implicar un riesgo de seguridad para los sistemas de información.		
Objetivos: Detectar posibles ataques o mal funcionamiento de la rede de datos que pudiera afectar a la seguridad de los sistemas de información y por tanto a los datos de la compañía.		
Responsable: • CIO	*Miembros implicados:* • CEO • CISO • CFO	

Mejoras Técnicas

Código: **MT-5**	*Proyecto:* **Auditoría PenTest**	
Presupuesto: 23.000 euros	*Inicio: 7/1/2019*	*Fin: 8/2/2019*
Controles Seguridad en las telecomunicaciones (13.1, 13.2) Adquisición, desarrollo y mantenimiento de los sistemas de información (14.1, 14.2)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Realización de una auditoría técnica de seguridad sobre los sistemas expuestos a Internet, y otra sobre servicios internos que pudieran suponer un riesgo de seguridad.		
Objetivos: Detectar posibles vulnerabilidades técnicas tanto en red interna como externa.		
Responsable: • CIO	*Miembros implicados:* • CEO • CISO • CFO	

Mejoras Técnicas

Código: **MT-6**	*Proyecto:* **Auditoría de código de los sistemas de información**	
Presupuesto: 175.000 euros	*Inicio: 3/12/2018*	*Fin: 31/5/2019*
Controles Seguridad en la operativa (12.5) Adquisición, desarrollo y mantenimiento de los sistemas de información (14.1, 14.2)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Auditoría de código de los sistemas de información.		
Objetivos: Detectar posibles amenazas derivadas de errores de programación, mala praxis u obsolescencia tecnológica.		
Responsable: • CIO	*Miembros implicados:* • CEO • CISO • CFO	

Mejoras Técnicas

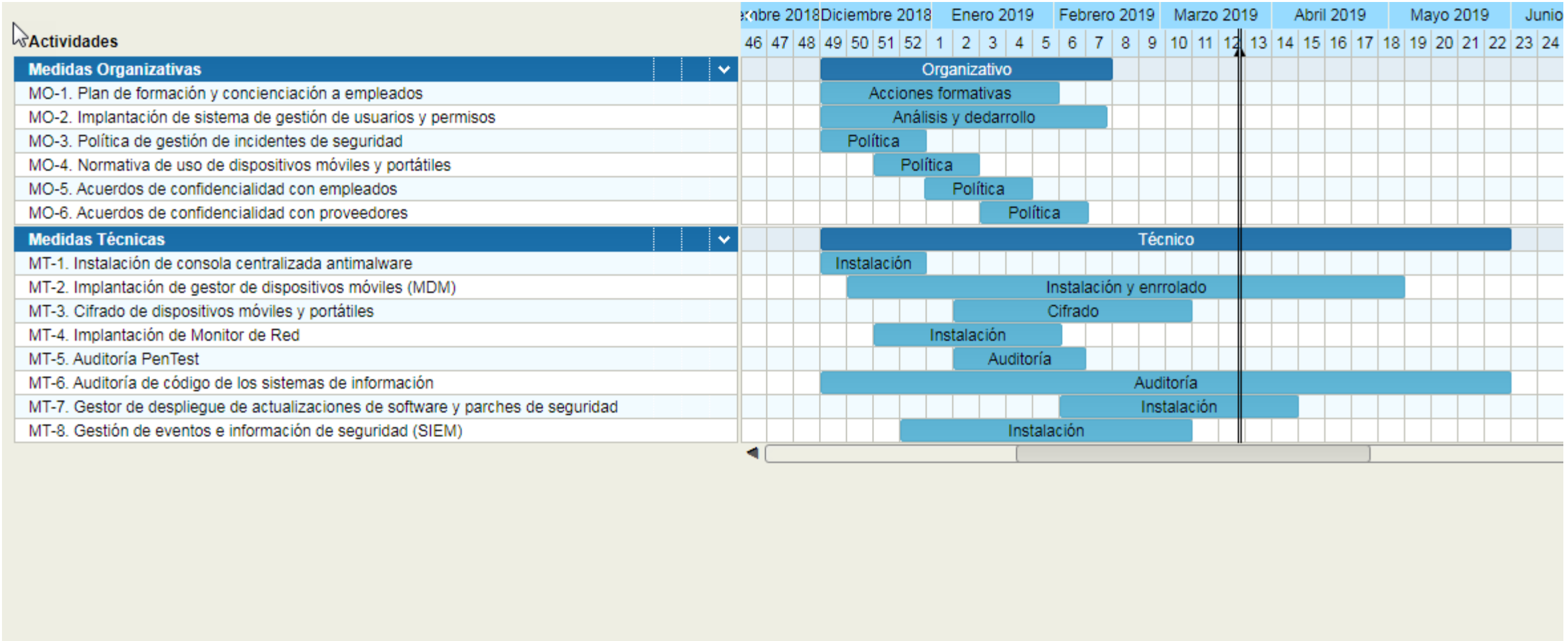
Código: **MT-7**	*Proyecto:* **Gestor de despliegue de actualizaciones de software y parches de seguridad**	
Presupuesto: 9.000	*Inicio: 4/2/2019*	*Fin: 5/4/2019*
Controles Seguridad en la operativa (12.6) Adquisición, desarrollo y mantenimiento de los sistemas de información (14.2)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Instalación y configuración de un gestor de actualizaciones de software y parches de seguridad. Este trabajo se viene haciendo de manera muy manual con el consiguiente riesgo.		
Objetivos: Tener el parque de PCs y servidores completamente actualizados con las versiones más recientes de software, así como parches de seguridad de SO.		
Responsable: • CIO	*Miembros implicados:* • CEO • CISO • CFO	

Mejoras Técnicas

Código: **MT-8**	*Proyecto:* **Gestión de eventos e información de seguridad (SIEM)**	
Presupuesto: 12.000 Euros	*Inicio: 24/12/2018*	*Fin: 8/3/2019*
Controles Control de accesos (9.4)	*Activos afectados:* • Navision • ProPlan365 • Portal del Empleado • Guardian365 • PeopleSoft • MasterCentral • Exchange/SharePoint	
Descripción: Instalación y configuración de un correlador de eventos de los distintos sistemas (red, servidores, software, etc.) de manera que se pueda detectar cualquier comportamiento extraño que pueda suponer un riesgo para la compañía.		
Objetivos: Detectar de manera casi instantánea cualquier intrusión u otra anomalía que pudiera suponer un riesgo.		
Responsable: • CIO	*Miembros implicados:* • CEO • CISO • CFO	

Proyecto propuestos tras el Análisis de Riesgos

Cronograma de proyectos a Marzo de 2019



Estado Actual

Finalizados

- MO-1. Plan de formación y concienciación a empleados
- MO-2. Implantación de sistema de gestión de usuarios y permisos
- MO-3. Política de gestión de incidentes de seguridad
- MO-4. Normativa de uso de dispositivos móviles y portátiles
- MO-6. Acuerdos de confidencialidad con proveedores
- MT-1. Instalación de consola centralizada antimalware
- MT-3. Cifrado de dispositivos móviles y portátiles
- MT-4. Implantación de Monitor de Red
- MT-5. Auditoría PenTest
- MT-8. Gestión de eventos e información de seguridad (SIEM)

Pendientes

- MT-2. Implantación de gestor de dispositivos móviles (MDM)
- MT-6. Auditoría de código de los sistemas de información
- MT-7. Gestor de despliegue de actualizaciones de software y parches de seguridad

Seguridad 365

Gracias

UOC
Universitat Oberta de Catalunya

UAB
Universitat Autònoma de Barcelona

UNIVERSITAT ROVIRA i VIRGILI

UIB
Universitat de les Illes Balears