Propuesta para la organización y gestión de un servicio de seguridad de la información en pymes

TRABAJO FIN DE GRADO
GRADO DE INGENIERÍA INFORMÁTICA
JUNIO 2020

Alumno: D. Francisco Javier de la Fuente Cagigós

Universitat Oberta de Catalunya
Estudios de Informática, Multimedia y Telecomunicación

Índice

Resumen

- Aumenta la sensibilización en las pymes pero desconocen cómo deben proceder en materia de Seguridad de la Información.
- Objetivo. Facilitar a las pymes una propuesta de organización y gestión de un servicio de seguridad de la información.
- Consecuencia. Estrategia alineada con negocio, aumentar la confianza de los clientes, mitigar la exposición ante posibles sanciones por pérdida de datos o tratamiento indebido, mayor grado de competitividad.

Descripción del problema

¿Cuál es el estado de la Seguridad de la Información en las pymes?

Pymes
99,8%

- Las pymes son objetivo de ataques para acceder a empresas más grandes.
- La mayoría únicamente cuentan con un antivirus o un cortafuegos para protegerse.

¿Qué sensación tienen los clientes sobre la seguridad y protección que se aplica a sus datos?

Preocupados por la protección de sus datos

- Preocupación de cómo se tratan sus datos.
- Preocupación por el cumplimiento legislativo.
- Preocupación por las medidas de seguridad.

Descripción del problema

¿Qué impacto tiene sobre las pymes?

- Pérdida de confianza de los clientes y reputación de marca.
- Dificultad en los equipos de fuerza de ventas para vender.
- Miedo de sanción o investigación por parte de la Agencia de Protección de Datos.

¿Qué medidas pueden adoptarse por parte de las pymes ?

- La Seguridad como un servicio.
- Medidas en los procesos de negocio.
- Gestión de la Seguridad de la Información.
- Definir cómo debe ser la organización.

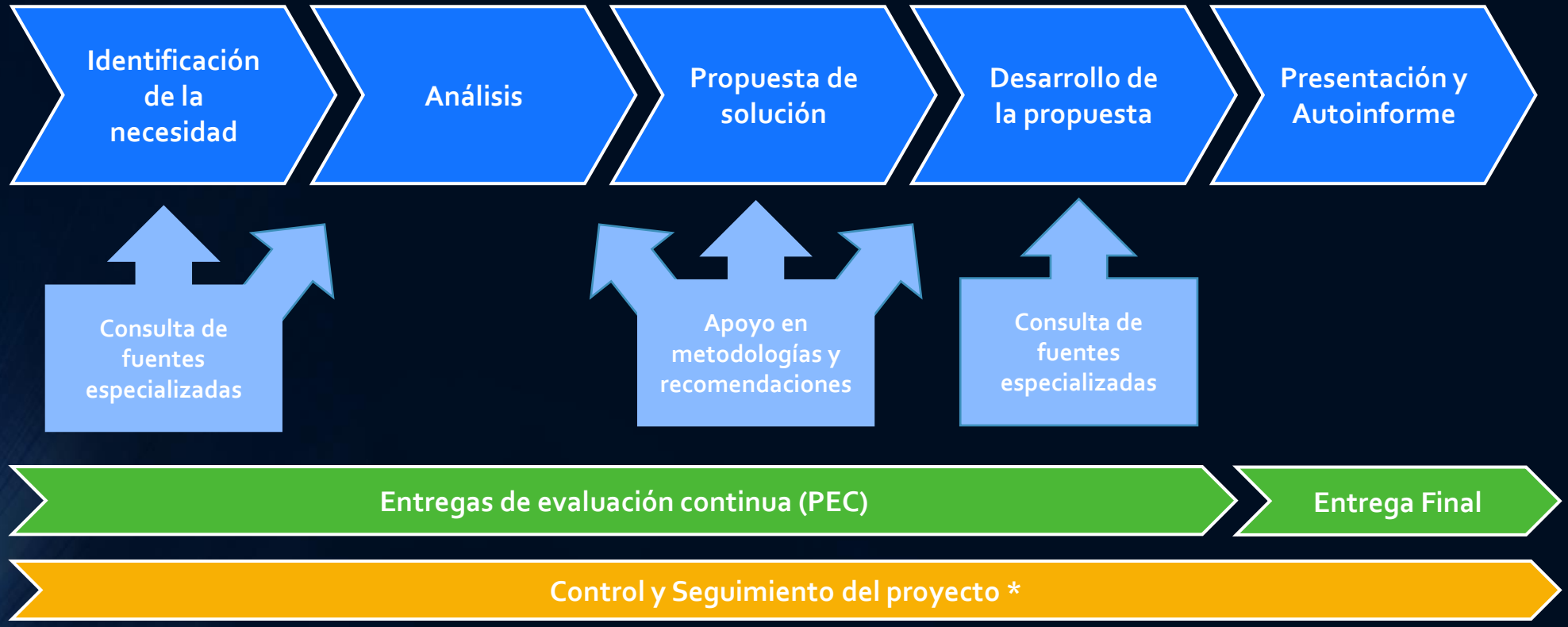
Confidencialidad, integridad y disponibilidad de los datos.

Objetivos

- Definir las características, estructura y gestión que debe tener un servicio de Seguridad de la Información que permita preservar la confidencialidad, la integridad y la disponibilidad de los datos de los clientes.
- Definir cómo debe ser la relación con el resto de las áreas de la empresa.
- Definir una estrategia de relación con servicios de terceros en cuanto a nivel de cumplimiento (RGPD) y en materia de Seguridad de la Información .

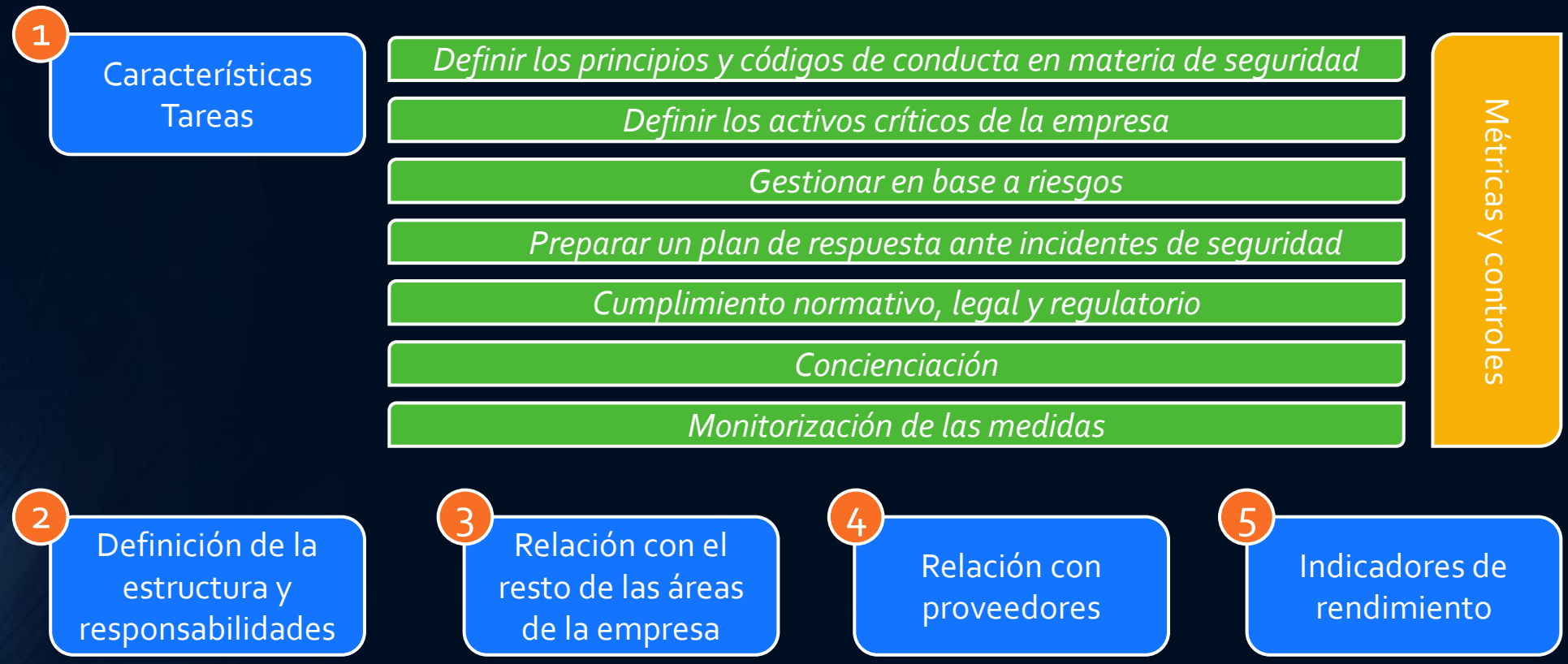
Estos objetivos tienen como finalidad mejorar la confianza de los clientes, conseguir un mayor nivel de fidelización y aumentar la competitividad de las *pymes.*

Pasos seguidos



* The PMBOK guide . Ciclo de vida de la administración de proyectos (Inicio, Planificación, Ejecución, Control, Cierre)

Solución propuesta



Solución propuesta

1. Características Tareas
2. Definición de la estructura y responsabilidades
3. Relación con el resto de las áreas de la empresa
4. Relación con proveedores
5. Indicadores de rendimiento

Definir los principios y códigos de conducta en materia de seguridad

- Declaración de intenciones de qué hacer.
- Respaldo de la alta dirección.
- Alineadas con la estrategia de Negocio.
- Políticas generales PD y Seguridad de la Información .
- Normativas (contraseñas, control de accesos, uso de los equipos de trabajo, etc.)

Definir los activos críticos de la empresa

- Activo: "*Recurso que tiene algún valor para la empresa y por tanto debe protegerse de potenciales riesgos*" *
- Clasificar los activos (valor, legal, sensibilidad o criticidad).

* Definicón en metodología MAGERIT v3 para el Análisis y Gestión de Riesgos de los Sistemas de Información .

Solución propuesta

1. Características Tareas
2. Definición de la estructura y responsabilidades
3. Relación con el resto de las áreas de la empresa
4. Relación con proveedores
5. Indicadores de rendimiento

Gestionar en base a riesgos

- Riesgos de Negocio.
- Riesgos en base a integridad, confidencialidad y disponibilidad
- Definir un umbral de riesgo.

Riesgo = *Impacto* x *Probabilidad*

PROBABILIDAD	IMPACTO: Bajo	Medio	Alto
Baja	*Muy bajo*	Bajo	Medio
Media	Bajo	Medio	*Alto*
Alta	Medio	*Alto*	*Muy alto*

Preparar un plan de respuesta ante incidentes de seguridad

- Minimizar el tiempo de respuesta ante un incidente, contener los daños y buscar una solución.
- Respaldo de la alta dirección.
- Equipo de respuesta.
- En conocimiento de todos los empleados y proveedores.

Solución propuesta

1. Características Tareas
2. Definición de la estructura y responsabilidades
3. Relación con el resto de las áreas de la empresa
4. Relación con proveedores
5. Indicadores de rendimiento

Cumplimiento normativo, legal y regulatorio

- Trabajo conjunto con otras áreas (Compliance, Auditoría, Jurídico).
- Ayudar a implementar las medidas.
- Identificación y gestión de los riesgos.

Concienciación

- **52%** de las empresas señalan al empleado como vector de ataque.
- Concienciar no es solo cosa del dpto. de Seguridad.
- Desarrollo de las habilidades.
- Constancia.

Solución propuesta

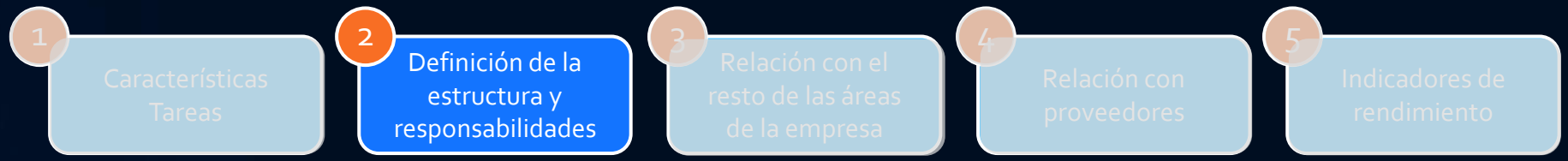
1. Características Tareas
2. Definición de la estructura y responsabilidades
3. Relación con el resto de las áreas de la empresa
4. Relación con proveedores
5. Indicadores de rendimiento

Monitorización de las medidas

- Seguimiento del desempeño, identificar áreas de mejora o anticiparse a posibles incidentes.
- Definición de indicadores.

Tarea	Métrica/Control	Objetivo de cumplimiento	Umbral de aceptación
Definir los principios y códigos de conducta en materia de seguridad	El detalle de posibles métricas aplicables a cada una de las políticas está detallado en la tabla *"Tabla 2. Definición de las políticas mínimas recomendadas a definir por una empresa"*. De forma generalizada a todas las políticas se pueden aplicar las siguientes:		
	Estado de revisión de las políticas	Revisión anual de todas las políticas	Revisión anual de al menos las políticas generales (seguridad y protección de datos)
	Porcentaje de áreas que conocen y aplican las políticas	100% de las áreas de la empresa	100% de las áreas que traten algún activo identificado como crítico
Definir los activos críticos de la empresa	% de activos que cumplen las políticas de Seguridad	100% de los activos en producción	70% de los activos en producción
	% de activos críticos que cumplen las políticas de Seguridad	100% de los activos en críticos	70% de los activos críticos
Gestionar en base a riesgos	% de activos críticos que cumplen las políticas de Seguridad para mitigar los riesgos y mantener los riesgos en niveles aceptables según el umbral definido	El 100% de los activos críticos deben estar dentro de los niveles aceptables según el umbral definido	Cumplimiento en activos con el riesgo más alto (probabilidad e impacto altos).
	% de áreas para las cuales se ha implantado una estrategia global para mantener los riesgos de Seguridad de la Información por debajo del umbral definido	Implantación de la estrategia global en el 100% de las áreas de la empresa	Implantación de la estrategia global en las áreas identificadas con mayor riesgo bien por tratar con información estratégica o bien por el uso de información sensible
Preparar un plan de respuesta ante incidentes de seguridad	Número de incidentes, su gravedad y estado	Tener en estado de resueltos el 90% de los incidentes, independientemente de su gravedad	Tener en estado de resueltos el 70% de los incidentes identificados como graves
	Número de incidentes que afectan a la Protección de Datos y estado	Cero incidentes comunicados a la Agencia de Española de Protección de	Cero incidentes comunicados a la Agencia de Española de Protección de

Solución propuesta



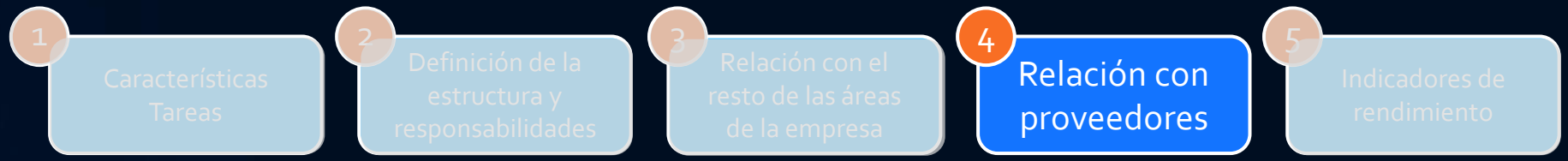
- Responsable de Seguridad de la Información.
  - *Posición interna.*
  - *Externalizado.*
- Organizativamente (TI, COO o CRO, CEO)
- Responsabilidades:
  - *Gestión operativa.*
  - *Alineamiento con las necesidades estratégicas y de Negocio.*
  - *Asegurar cumplimiento normativo y de regulaciones.*
  - *Definición de políticas y procedimientos.*
  - *Gestión del riesgo.*
  - *Definir un Plan de respuesta de incidentes.*
  - *Definición de indicadores y Monitorización.*
  - *Concienciación.*
  - *Mejora continua.*

Solución propuesta

1. Características Tareas
2. Definición de la estructura y responsabilidades
3. **Relación con el resto de las áreas de la empresa**
4. Relación con proveedores
5. Indicadores de rendimiento

- Relación fundamental e importante.
- La seguridad debe ponerse en práctica en el día a día.
- Cumplimiento de políticas y normativas.
- Procesos afectados:
  - *Gestión del cambio.*
  - *Gestión de la configuración.*
  - *Pruebas.*
  - *Protección de datos.*
  - *Auditoría.*
  - *Desarrollo.*
  - *Diseño de nuevas arquitecturas y definición de nuevos productos de Negocio.*
  - *Proceso de altas y bajas de RR.HH.*

Solución propuesta



- Garantizar la calidad necesaria y deseable en materia de Seguridad de la Información .
- Acuerdos con claúsulas o anexos con requisitos (ANEXO A y B del TFG).
  - *Requisitos en el tratamiento de datos personales.*
  - *Requisitos de seguridad a proveedores.*
- Medir el cumplimiento mediante auditorías periódicas tanto por cumplimiento normativa o legal, como para los acuerdos del contrato.

Solución propuesta

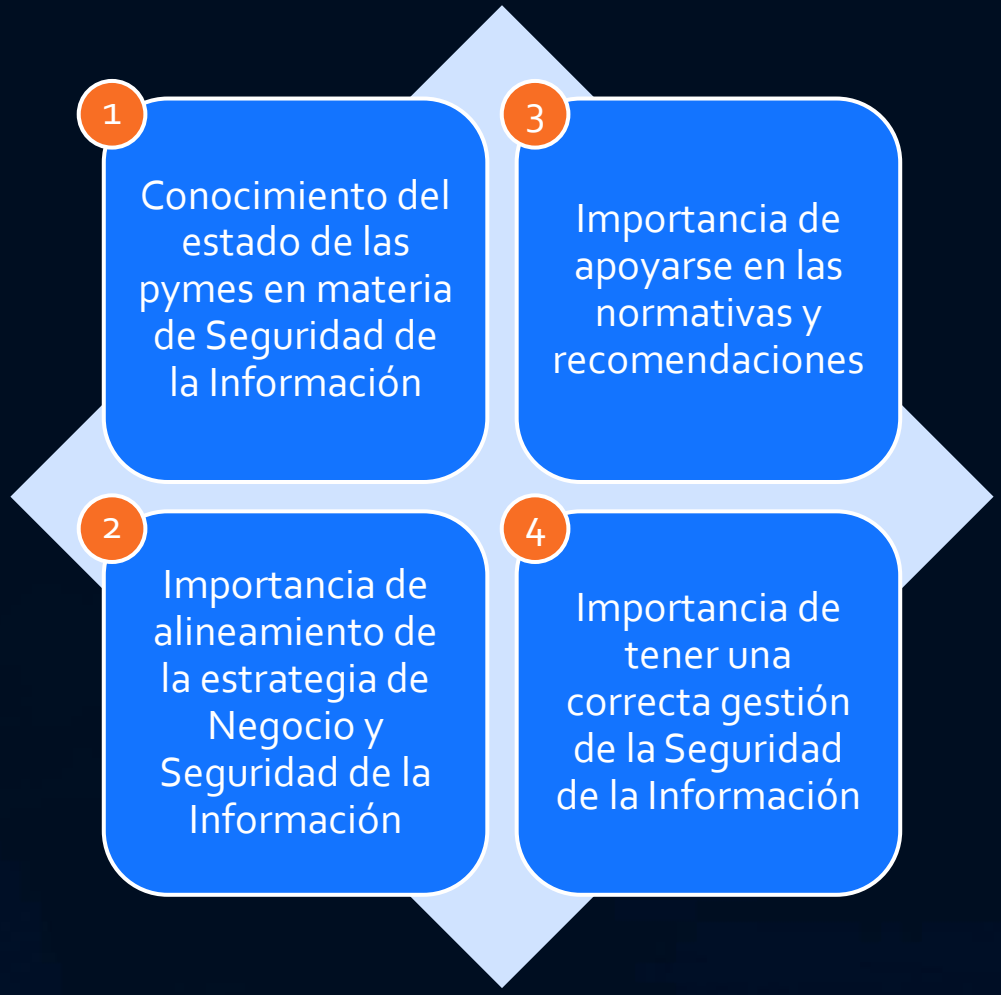
1. Características Tareas
2. Definición de la estructura y responsabilidades
3. Relación con el resto de las áreas de la empresa
4. Relación con proveedores
5. Indicadores de rendimiento

- Medir el rendimiento de las tareas con el objetivo de validar y mejorar los procesos y controles implantados.
- Definición de los indicadores.
  - Estado de los parches de seguridad en servidores y equipos personales.
  - % de correo SPAM, Phishing, Malware.
  - Número de incidentes de seguridad de la información.

Resultado final

- Una propuesta de cómo debe ser la organización y la gestión de un servicio de seguridad de la información en pymes, la relación con terceros y con las áreas internas de la empresa; así como, la adaptación para el cumplimiento en materia de protección de datos.
- Anexo, propuesta de política interna en materia de protección de datos.
- Anexo, propuesta de política interna en materia de seguridad.
- Anexo, propuesta (para anexar a contrato) de requerimientos a terceros en materia de seguridad de la información.
- Anexo, propuesta (para anexar a contrato) de requerimientos en el tratamiento de protección de datos personales.

Conclusiones



Conclusiones

Recomendación a pymes

- Concienciación al empleado, es el eslabón más débil de la cadena.
- Nombrar un responsable de Seguridad de la Información (interno o externo).
- Ejecución de auditorias de forma periódica.

Otras líneas de investigación

- Implementación del servicio de Seguridad.
- Definición de un plan director de Seguridad.
- Implantación de la normativa ISO 27001 o de gobierno según COBIT 5.

Bibliografía

- ISACA, CSX Cybersecurity Fundamentals. Study Guide, 2nd Edition, ISACA, 2017.
- MAGERIT v3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Octubre 2012 [En línea] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XFSfLlVKiUk [Consultado: marzo 2020]
- ISACA. COBIT 5 para Seguridad de la Información. 2012, Ed. ISACA.
- R. Mulcahy y L. Diethelm, Preparación para el examen PMP. 7th edición (PMBOK 4th Edition), RMC Publications, Inc, 2011.
- RGPD. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [En línea] https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=es [Consultado: abril de 2020]
- Google and The cocktail analysis, «Panorama actual de la Ciberseguridad en España. Retos y oportunidades para el sector público y privado,» 19 octubre 2019. [En línea]. Available: https://drive.google.com/file/d/18TNjaDus-lrSl5gL5Wt-Z4DOsKXtQ46m/view. [Último acceso: febrero 2020].
- LEGALTODAY, «El 81% de los consumidores, preocupados por la Seguridad en sus dispositivos,» 1 octubre 2020. [En línea]. Available: http://www.legaltoday.com/actualidad/noticias/el-81-de-los-consumidores-preocupado-por-la-seguridad-en-sus-dispositivos. [Último acceso: febrero 2020].
- M. Á. Moreno, «Diario online La Vanguardia. Las pymes dejan muchas veces la ciberseguridad a un lado, dice Deepak Daswani,» EFE, 17 octubre 2018. [En línea]. Available: https://www.lavanguardia.com/vida/20181217/453601860042/las-pymes-dejan-muchas-veces-la-ciberseguridad-a-un-lado-dice-deepak-daswani.html. [Último acceso: febrero 2020].
- AEPD y CEPYME, «Encuesta sobre el grado de preparación de las empresas españolas ante el reglamento general de protección de datos. Informe ejecutivo,» octubre 2019. [En línea]. Available: https://www.aepd.es/sites/default/files/2019-10/estudio-proteccion-de-datos-aepd-cepyme.pdf. [Último acceso: febrero 2020].
- J. G. Fernández, «Incibe: "Los hackers atacan a las pymes para llegar a las grandes empresas",» Diario Expansión edición online, 1 diciembre 2019. [En línea]. Available: https://www.expansion.com/economia-digital/protagonistas/2019/12/01/5ddfc152468aebc4718b46b5.html. [Último acceso: marzo 2020].
- CincoDías (El País economía), «Las pymes pasan bastante de gastarse dinero en ciberseguridad,» 24 mayo 2019. [En línea]. Available: https://cincodias.elpais.com/cincodias/2019/05/23/pyme/1558612494_142435.html. [Último acceso: marzo 2020].
- MAGERIT v3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Octubre 2012 [En línea] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XFSfLlVKiUk [Consultado: marzo 2020]

Gracias