UAB Universitat Autònoma de Barcelona

UOC www.uoc.edu

Universitat Rovira i Virgili

Máster Interuniversitario en Seguridad de las TIC (MISTIC)

Plan de Implementación de la ISO/IEC 27001:2013

RecycleSA

Presentación a Dirección

Autor: Cristóbal Garrido Camargo
Dirección: Antonio José Segovia Henares

Fecha: 21/12/2018

Seguridad de la información

Problema.

Seguridad de la información

EUROPA 20:58 20.12.2018 (actualizada a las 21:03 20.12.2018) URL corto 1 0 2

LONDRES (Sputnik) — El Gobierno del Reino Unido ha responsabilizado a China de una oleada de persistentes ataques cibernéticos que tendría como objetivo la sustracción de información confidencial comercial y de propiedad intelectual.

Hacer medicina "a ciegas": los ciberataques ponen en jaque a la medicina actual y no estamos seguros de estar preparados

MEDICINA Y SALUD

La sanidad británica se ha puesto en jaque por el ataque de ransomware y, segú mismos médicos, los pr serios. ¿Es

SISTEMAS DE CONTROL INDUSTRIAL (ICS) PRINCIPAL OBJETIVO DE LOS CIBERATAQUES

Seguridad de la información

La polémica por el espionaje de McLaren a Ferrari marcó al «circo»

Mike Coughlan, ingeniero de McLaren, se fue a fotocopiar un dossier con todas las especificaciones técnicas de los bólidos de Ferrari de esta temporada. El documento, de varios cientos de folios, se

europapress / economía finanzas / finanzas

El Banco de España sufre un ciberataque que impide el acceso a su web desde servidores externos

incibe-cert_

Alerta Incidentes Se

Inicio / Alerta Temprana / Bitacora Ciberseguridad / APT "dragonfly" en Sistemas de Control Industrial

APT "dragonfly" en Sistemas de Control Industrial

30/06/2014

La compañía de seguridad Symantec ha publicado un reporte sobre una campaña de malware especialmente enfocado a Sistemas de Control Industrial utilizados en el sector energético, aunque también se ha detectado en el sector farmacéutico.

Esta APT afecta especialmente a países europeos y utiliza varios componentes de tipo RAT (Remote Access Tool) para infectar y controlar remotamente los equipos afectados.

Este malware se distribuía a través de páginas webs de fabricantes de software para sector energético previamente modificadas por los atacantes, tal y como también informo la compañía F-Secure.

INTERECONOMIA.COM

WannaCry costó más de 1.000 millones de dólares a las empresas afectadas

Seguridad de la información

Obtención de beneficios económicos

En 2017 también se llevaron a cabo ataques con el objetivo de obtener rendimiento económico. Para ello, se emplearon distintos métodos.

Fraude al CEO

Los delincuentes intentan que el departamento financiero de una empresa realice transacciones económicas utilizando nombres de dominio similares al de la organización en cuestión.

Malware COBALT[2]

Envío de correos electrónicos a empleados de bancos con un archivo adjunto malicioso que permitía tener acceso a la red bancaria interna e infectar los servidores que controlan los cajeros automáticos.

Ciberpiratería

En Italia, la policía detuvo en 2017 a dos individuos sospechosos de ciberpiratería, que habrían realizado inversiones basándose en información robada.

Ciberespionaje

Esta problemática ha afectado durante 2017 a todos los países de nuestro entorno occidental. El ciberespionaje representa una amenaza que confirma el interés de los atacantes por obtener **información sensible** de las empresas e instituciones tanto españolas como occidentales.

Disrupción de sistemas

La novedad en este tipo de ataques radica en el empleo de **dispositivos de Internet of Things (IoT)** de consumidores finales para perpetrar significativos ataques DDoS[1]. Así lo hicieron la botnet *Mirai* o la botnet *LizardStresser*, que infectaron decenas de miles de dispositivos de consumidores.

De la misma forma, las redes de energía eléctrica de Arabia Saudí, así como ciertas agencias gubernamentales también fueron víctimas de ciberataques en 2017, empleándose para ello el código dañino *Shamoon*.

Ciberconflictos

Seguridad de la información

Conceptos

Seguridad de la información. Conceptos

- **Activo**

  Es cualquier elemento al cual se le asigna un valor y por lo tanto requiere protección.
- **Amenaza.**

  Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.
- **Riesgo**

  Probabilidad de que una amenaza determinada se materialice produciendo un impacto negativo sobre los activos
- **Salvaguarda**

  Procedimiento o mecanismo tecnológicos que reduce el riesgo.

Seguridad de la información. Dimensiones

- **Confidencialidad**

  Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]

- **Disponibilidad**

  Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]

- **Integridad**

  Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]

- **Autenticidad**

  Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

- **Trazabilidad**

  Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]

Seguridad de la información. Conceptos

- **Seguridad de la Información**

  Es el conjunto de medidas preventivas y reactivas que permite resguardar y proteger la información. Se ocupa de la información **en todas sus formas** (**oral, impresa, electrónica**,…), a diferencia de la seguridad informática, que se ocupa únicamente de la seguridad de los sistemas de información.

- **SGSI**

  Es la abreviatura utilizada para referirse a un **Sistema de Gestión de la Seguridad de la Información**. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

Seguridad de la información

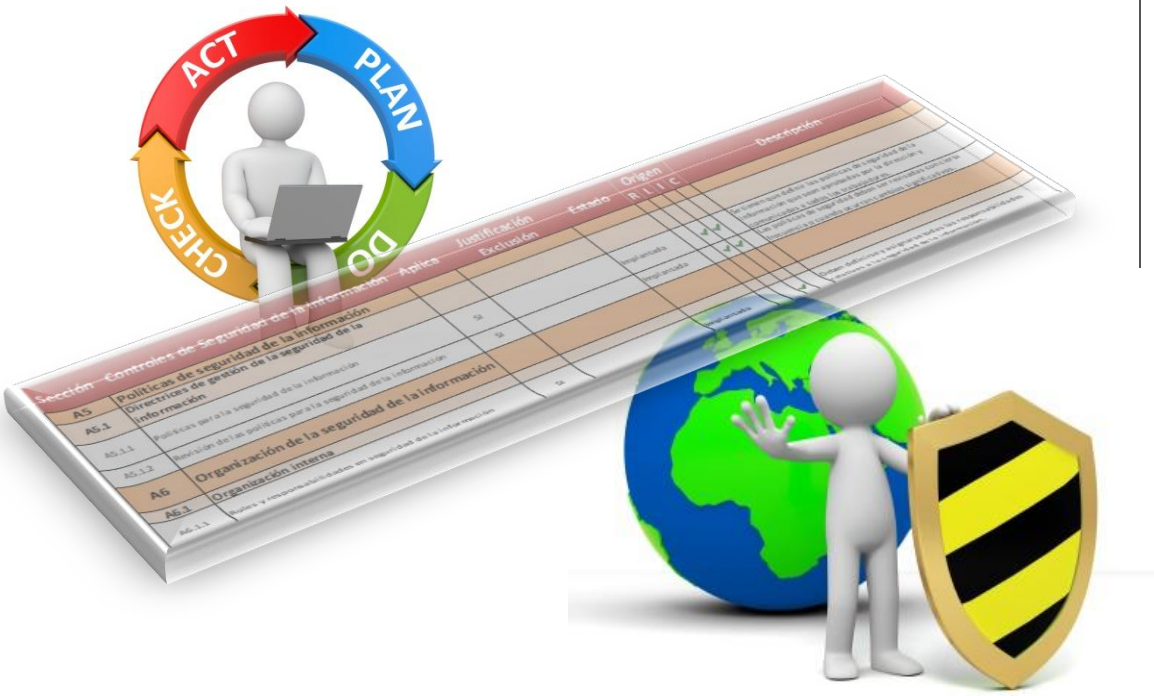
Solución.

Implementación de la ISO/IEC 27001:2013
RecycleSA

Necesidad.

Metodología.

Situación actual.



Necesidad

- La información es un activo importante que es necesario proteger.
- Es necesario implantar un Sistema de Gestión de Seguridad de la Información que la proteja adecuadamente.
- La norma ISO/IEC 27001:2013 es un estándar ampliamente reconocido que permite la certificación de la organizaciones.

Implantar un Sistema de Gestión de la Seguridad basado en la norma ISO/IEC 27001:2013

Necesidad

- Concienciación de la necesidad de proteger.
- Compromiso de la Alta Dirección.
- Formación a todos los niveles y en todos los estamentos.

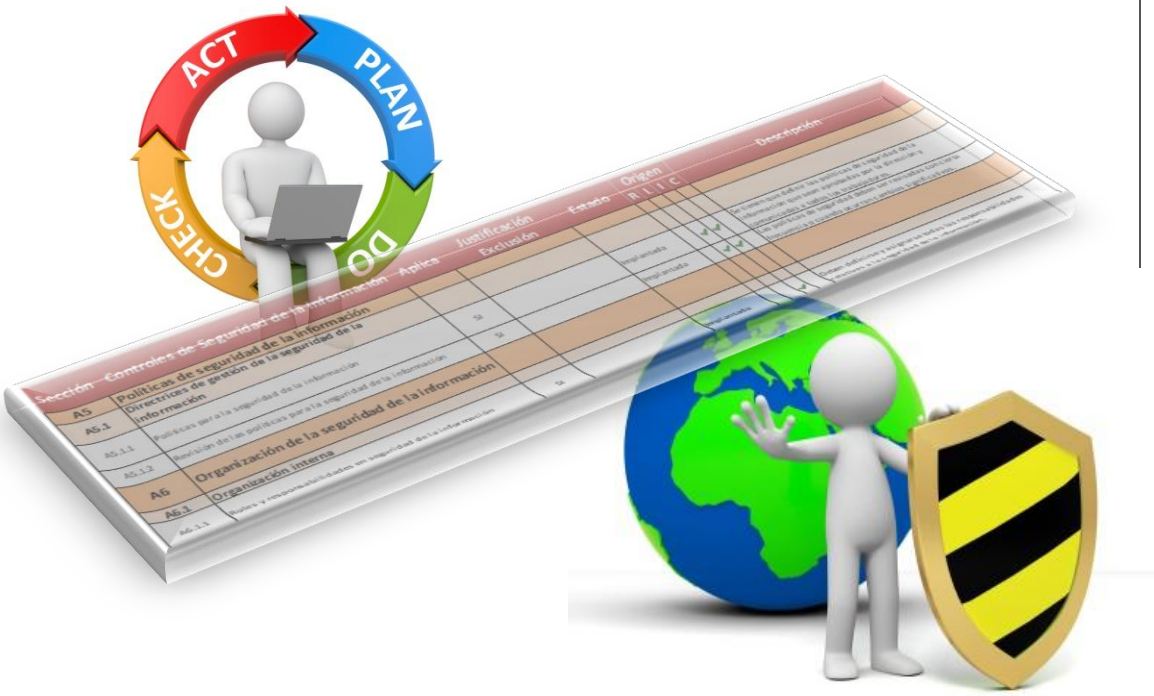
La seguridad de la información incumbe a TODA LA ORGANIZACIÓN

Implementación de la ISO/IEC 27001:2013
RecycleSA

Necesidad.

Metodología.

Situación actual.



Metodología

La implantación del SGSI se ha llevado a cabo mediante la ejecución de la siguientes fases:

1. Situación Actual.
2. Sistema de gestión documental.
3. Análisis de riesgos.
4. Propuestas de Proyectos.
5. Auditoría de Cumplimiento.
6. Conclusiones y presentación de resultados.

Metodología: Situación actual

1. Contextualización:
   - Estructura organizativa.
   - Estructura servicios TI.
   - Usuarios y sedes.
   - Infraestructura tecnológica.
   - Puesto de trabajo y dispositivos móviles.
   - Aplicaciones corporativas.
   - Infraestructura y redes.
   - Alcance SGSI
2. Definición de objetivos.
3. Análisis diferencial.

Metodología. Sistema gestión documental

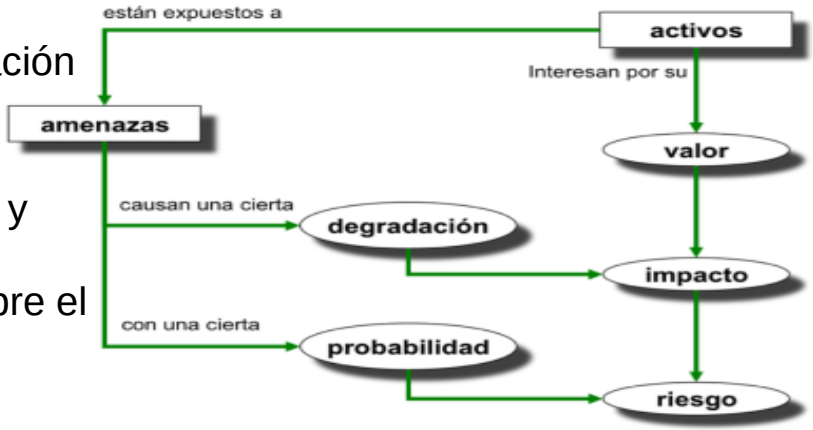
Documentos desarrollados

- Política de Seguridad.
- Procedimiento de Auditorías Internas.
- Gestión de Indicadores.
- Procedimiento de Revisión por la Dirección.
- Gestión de Roles y Responsabilidades.
- Metodología de Análisis de Riesgo: Magerit.
- Declaración de Aplicabilidad

Metodología. Análisis de riesgos

Metodología: Magerit

- Determinar los **activos** relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio supondría su degradación
- Determinar a qué **amenazas** están expuestos aquellos activos
- Determinar qué **salvaguarda**s hay dispuestas y cuán eficaces son frente al riesgo
- Estimar el **impacto**, definido como el daño sobre el activo derivado de la materialización de la amenaza
- Estimar el **riesgo**, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.



Metodología. Análisis de riesgos

Estimación inicial de riesgos por activo

Tipo Activo	ID Activo	Activo	Riesgo A	Riesgo C	Riesgo I	Riesgo D	Riesgo T
Instalaciones [L]	[L.1]	CPD	MB	MB	MB	MA	MB
	[L.2]	Sala Técnica Sede	MB	MB	MB	MA	MB
	[L.3]	Despacho Directivo	MB	MB	MB	M	MB
	[L.4]	Oficinas	MB	MB	MB	M	MB
Hardware [HW]	[HW.1]	Servidores hypervisor CPD	B	MA	A	MA	B
	[HW.2]	Firewall CPD	B	MA	A	MA	B
	[HW.3]	Swithes CPD	B	A	A	MA	B
	[HW.4]	Servidores hypervisor Sedes	B	A	M	A	B
	[HW.5]	Switches/routers Sedes	B	A	M	A	B
	[HW.6]	Puntos de acceso Wifi	B	A	M	M	B
	[HW.7]	PCs usuarios	B	A	M	A	B
	[HW.8]	Portátiles usuarios	B	A	M	A	B
	[HW.9]	Dispositivos móviles corporativos	B	A	B	M	B
	[HW.10]	Dispositivos móviles personales	B	A	B	M	B
	[HW.11]	Teléfonos IPs	B	B	B	M	B
Aplicaciones [SW]	[SW.1]	Software virtualizacion VMWare	A	MA	MA	MA	B
	[SW.2]	Sistema operativos Windows Server	A	MA	MA	MA	B
	[SW.3]	Sistema operativos Linux Server	A	MA	A	A	B
	[SW.4]	Software backup: Veeam backup	A	MA	MA	B	B
	[SW.5]	Sistema operativo Windows 7	A	A	M	A	B
	[SW.6]	Sistema operativo Windows 10	A	A	M	A	B
	[SW.7]	Sistema operativo android	M	A	M	M	B
	[SW.8]	Sistema operativo IOS	M	A	M	M	B
	[SW.9]	Directorio Activo Microsoft	A	A	MA	MA	B
	[SW.10]	BBDD Microsoft SQL Server	A	MA	MA	A	B
	[SW.11]	BBDD Oracle	A	MA	MA	MA	B
	[SW.12]	Microsoft SCCM	M	A	M	A	B
	[SW.13]	Herramienta de ticketing: OTRS	M	A	M	MA	B
	[SW.14]	Antivirus Symantec	M	M	A	A	B
	[SW.15]	Intranet corporativa	A	MA	A	A	B
	[SW.16]	Web corporativa	A	A	MA	A	B
	[SW.17]	SAP	A	MA	MA	MA	B
	[SW.18]	Navision	A	MA	MA	MA	B
	[SW.19]	Contaplus	A	A	A	A	B
	[SW.20]	Software puesto usuario: office 365, antivirus, acrobat	M	A	A	A	B
	[SW.21]	Aplicaciones Office 365: Correo, one drive, skype,...	A	MA	A	A	B
	[SW.22]	Aplicaciones Sharepoint Office 365	A	MA	A	A	B

Tipo Activo	ID Activo	Activo	Riesgo A	Riesgo C	Riesgo I	Riesgo D	Riesgo T
Datos/Información [D]	[D.1]	Servidores de ficheros corporativos	MA	MA	MA	A	A
	[D.2]	Bases de datos ERPs: SAP, Navision, Contaplus	MA	MA	MA	MA	MA
	[D.3]	Bases de datos RRHH	MA	MA	MA	MA	MA
	[D.4]	LDAP: Directorio Activo Microsoft	A	A	MA	MA	A
	[D.5]	Copias de seguridad	A	MA	A	M	A
Comunicaciones [D]	[COM.1]	Red internet	A	MA	A	MA	B
	[COM.2]	Red MPLS	A	MA	A	MA	B
	[COM.3]	Red local CPD	A	MA	A	MA	B
	[COM.4]	Red local sedes	A	A	A	A	B
	[COM.5]	Red wifi invitados sedes	B	M	M	M	B
	[COM.6]	Red wifi movilidad sedes (usuarios VIP)	M	M	M	M	B
	[COM.7]	Red wifi usuarios	M	A	M	A	B
	[COM.8]	Red telefonía IP	B	B	B	A	B
	[COM.9]	Red telefonía móvil	B	B	B	MA	B
Servicios [S]	[S.1]	Servicio ERP	A	A	A	MA	A
	[S.2]	Servicio correo	A	A	A	MA	A
	[S.3]	Servicio de telefonía	B	M	B	MA	B
	[S.4]	Servicio de ficheros	A	A	A	A	A
	[S.5]	Servicio de acceso remoto	A	A	A	A	A
	[S.6]	Servicio de backup	A	A	A	A	A
Soportes de Información [M]	[M.1]	Almacenamiento CPD	B	MA	A	MA	B
	[M.2]	Almacenamiento Sedes	B	A	M	A	B
	[M.3]	Memorias USB	B	A	B	B	B
Equipamiento Auxiliar [AUX]	[AUX.1]	Sistema eléctrico	B	B	B	MA	B
	[AUX.2]	Aire acondicionado Salas técnicas	B	B	B	A	B
	[AUX.3]	Sistemas antiincendios	B	B	B	MA	B
	[AUX.4]	Cableado LAN	B	B	B	MA	B
Personal [P]	[P.1]	Personal Dirección: CEO, Auditor, Director Financiero	B	B	B	MA	B
	[P.2]	Personal TI	B	B	B	MA	B
	[P.3]	Personal Proveedor TI	B	B	B	A	B
	[P.4]	Resto de personal	B	B	B	M	B

Metodología. Proyectos

Proyectos propuestos para mitigar los riesgos de seguridad.
En base a:

- Análisis de riesgos, amenazas, análisis diferencial.
- Recursos TI limitados.
- Espacio temporal un año

Ámbto	ID	Proyecto
Tecnológico	PRY1	Migración infraestructura CPD a modelo IaaS
	PRY2	Securización dispositivos portátiles
	PRY3	Eliminación infraestructura de servidores sedes
	PRY4	Implantación solución MDM
Organizativo/Gestión	PRY5	Políticas de seguridad
	PRY6	Plan de Formación
	PRY7	Política de dispositivos móviles
	PRY8	Política y auditoría de control de accesos
	PRY9	Plan de continuidad de negocio
	PRY10	Procedimientos de gestión de incidentes de seguridad

Metodología. Auditoría de cumplimiento

Declaración de aplicabilidad

- Controles que aplican
- Origen del control
- Justificación su exclusión

Informe de auditoría

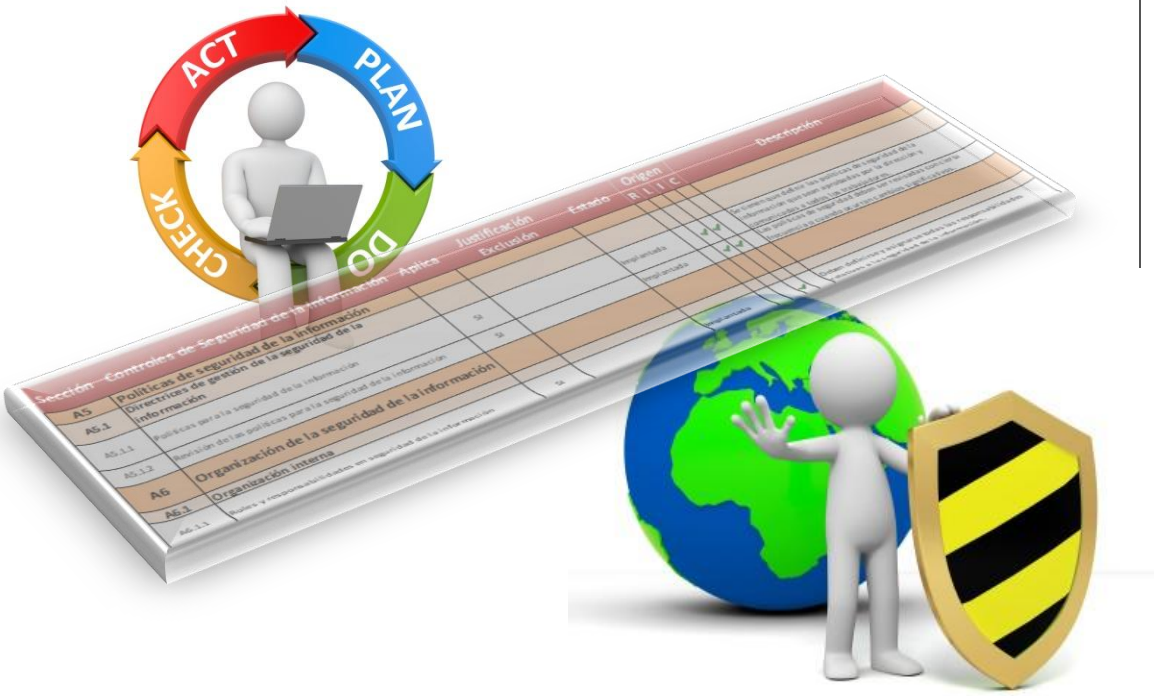
- Plan de auditoría.
- Registros de auditoría.
- Resultado de auditoria.
- Oportunidades de mejora.
- Planificación futura auditoría

Implementación de la ISO/IEC 27001:2013
RecycleSA

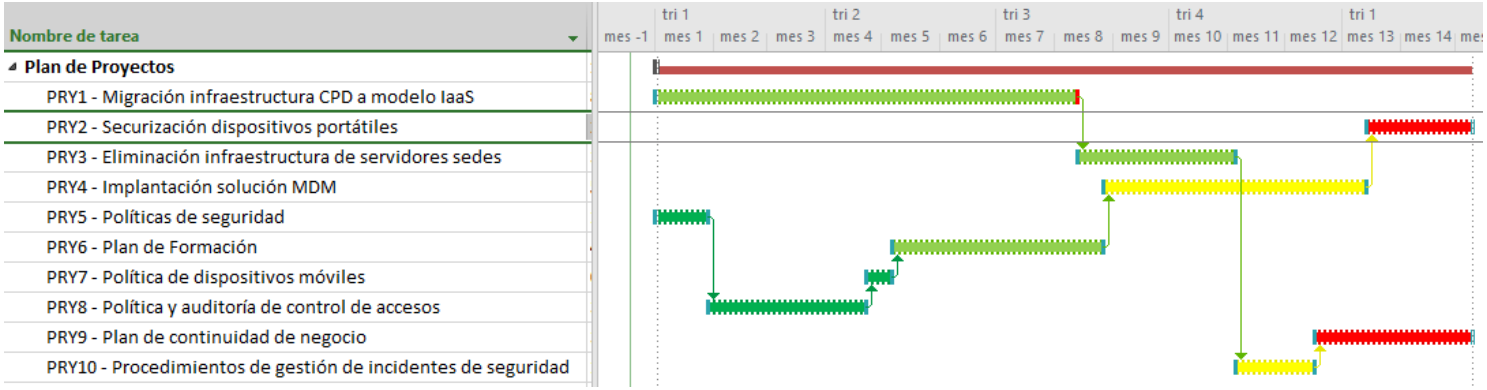
Necesidad.

Metodología.

Situación actual.



Situación actual. Estado proyectos



LEYENDA

- **Finalizado en plazo previsto**
- **Finalizado con retraso**
- **En curso**
- **No iniciado**

Situación actual. Evaluación de riesgos

Estimación actual de riesgos por activo

Tipo Activo	ID Activo	Activo	Riesgo A	Riesgo C	Riesgo I	Riesgo D	Riesgo T
Instalaciones [L]	[L.1]	CPD	MB	MB	MB	A	MB
	[L.2]	Sala Técnica Sede	MB	MB	MB	A	MB
	[L.3]	Despacho Directivo	MB	MB	MB	M	MB
	[L.4]	Oficinas	MB	MB	MB	M	MB
Hardware [HW]	[HW.1]	Servidores hypervisor CPD	B	A	A	A	B
	[HW.2]	Firewall CPD	B	A	A	A	B
	[HW.3]	Swithes CPD	B	A	A	A	B
	[HW.4]	Servidores hypervisor Sedes	B	A	M	A	B
	[HW.5]	Switches/routers Sedes	B	A	M	A	B
	[HW.6]	Puntos de acceso Wifi	B	A	M	M	B
	[HW.7]	PCs usuarios	B	A	M	M	B
	[HW.8]	Portátiles usuarios	B	A	M	M	B
	[HW.9]	Dispositivos móviles corporativos	B	A	B	M	B
	[HW.10]	Dispositivos móviles personales	B	A	B	M	B
	[HW.11]	Teléfonos IPs	B	B	B	M	B
Aplicaciones [SW]	[SW.1]	Software virtualizacion VMWare	A	MA	MA	A	B
	[SW.2]	Sistema operativos Windows Server	A	MA	MA	A	B
	[SW.3]	Sistema operativos Linux Server	A	MA	A	A	B
	[SW.4]	Software backup: Veeam backup	A	MA	MA	B	B
	[SW.5]	Sistema operativo Windows 7	A	A	M	A	B
	[SW.6]	Sistema operativo Windows 10	A	A	M	A	B
	[SW.7]	Sistema operativo android	M	A	M	M	B
	[SW.8]	Sistema operativo IOS	M	A	M	M	B
	[SW.9]	Directorio Activo Microsoft	A	A	MA	A	B
	[SW.10]	BBDD Microsoft SQL Server	A	MA	MA	A	B
	[SW.11]	BBDD Oracle	A	MA	MA	A	B
	[SW.12]	Microsoft SCCM	M	A	M	A	B
	[SW.13]	Herramienta de ticketing: OTRS	M	A	M	A	B
	[SW.14]	Antivirus Symantec	M	M	A	A	B
	[SW.15]	Intranet corporativa	A	MA	A	A	B
	[SW.16]	Web corporativa	A	A	MA	A	B
	[SW.17]	SAP	A	MA	MA	A	B
	[SW.18]	Navision	A	MA	MA	A	B
	[SW.19]	Contaplus	A	A	A	M	B
	[SW.20]	Software puesto usuario: office 365, antivirus,	M	A	A	M	B
	[SW.21]	Aplicaciones Office 365: Correo, one drive, sky	A	MA	A	A	B
	[SW.22]	Aplicaciones Sharepoint Office 365	A	MA	A	A	B

Tipo Activo	ID Activo	Activo	Riesgo A	Riesgo C	Riesgo I	Riesgo D	Riesgo T
Datos/Información [D]	[D.1]	Servidores de ficheros corporativos	A	A	A	M	M
	[D.2]	Bases de datos ERPs: SAP, Navision, Contaplus	A	A	A	A	A
	[D.3]	Bases de datos RRHH	A	A	A	A	A
	[D.4]	LDAP: Directorio Activo Microsoft	M	M	A	A	M
	[D.5]	Copias de seguridad	M	A	M	B	M
Comunicaciones [D]	[COM.1]	Red internet	M	A	M	A	MB
	[COM.2]	Red MPLS	M	A	M	A	MB
	[COM.3]	Red local CPD	M	A	M	A	MB
	[COM.4]	Red local sedes	M	M	M	M	MB
	[COM.5]	Red wifi invitados sedes	MB	B	B	B	MB
	[COM.6]	Red wifi movilidad sedes (usuarios VIP)	B	B	B	B	MB
	[COM.7]	Red wifi usuarios	B	M	B	M	MB
	[COM.8]	Red telefonía IP	MB	MB	MB	M	MB
	[COM.9]	Red telefonía móvil	MB	MB	MB	A	MB
Servicios [S]	[S.1]	Servicio ERP	M	M	M	M	M
	[S.2]	Servicio correo	M	M	M	M	M
	[S.3]	Servicio de telefonía	MB	B	MB	M	MB
	[S.4]	Servicio de ficheros	M	M	M	M	M
	[S.5]	Servicio de acceso remoto	M	M	M	M	M
	[S.6]	Servicio de backup	M	M	M	M	M
Soportes de Información [M]	[M.1]	Almacenamiento CPD	B	MA	A	MA	B
	[M.2]	Almacenamiento Sedes	B	A	M	A	B
	[M.3]	Memorias USB	B	A	B	B	B
Equipamiento Auxiliar [AUX]	[AUX.1]	Sistema eléctrico	B	B	B	MA	B
	[AUX.2]	Aire acondicionado Salas técnicas	B	B	B	A	B
	[AUX.3]	Sistemas antiincidencios	B	B	B	MA	B
	[AUX.4]	Cableado LAN	B	B	B	MA	B
Personal [P]	[P.1]	Personal Dirección: CEO, Auditor, Director Fina	B	B	B	A	B
	[P.2]	Personal TI	B	B	B	A	B
	[P.3]	Personal Proveedor TI	B	B	B	A	B
	[P.4]	Resto de personal	B	B	B	M	B

Situación actual. Objetivos alcanzados

- SGSI definido y puesto en marcha.
- Implicación en la Seguridad de toda la organización
- Mejorada formación y concienciación.
- Amenazas y riesgos identificados.

Mejora de la seguridad global conseguida

Situación actual. Aspectos pendientes

- Definir e implementar la política de seguridad de proveedores.
- Definir e implementar procedimientos de seguridad relativos a los recursos humanos.
- Corregir las no conformidades detectadas en la auditoría.
- Definir y desarrollar planes de formación específicos para el personal con responsabilidades en materia de seguridad de la información.

Mejora continua del SGSI

Plan de Implementación de la ISO/IEC 27001:2013

Gracias por su atención

Cristóbal Garrido Camargo