La Ciberseguridad como parte del nuevo paradigma de la seguridad

Área de Trabajo Ciberseguridad

Asociación Española de empresas de Seguridad

Dinamizando la Industria de la Seguridad

Dominios Ciberseguridad

Introducción

- Arquitectura de Seguridad: Activos IT, su configuración y conexión entre ellos y las redes.
- Desarrollos
- Riesgos de activos IT y salvaguardas: taxonomía de riesgos sobre los activos de la empresa y los mecanismos para prevenirlos o mitigarlos.
- Comunicación, Concienciación y Formación
- Inteligencia de amenazas
- Seguridad Física
- Gobernanza y Estándares: estructura jerárquica de políticas, planes y procesos así como los estándares y cuadros de mando que gestionan la compañía

Introducción

Etapas de estudio

Para la generación de la guía de buenas prácticas de la Asociación Española de Empresas e Seguridad (AES) se siguieron 3 etapas:

- Etapa 1: Definición del contexto
- Etapa 2: Medidas de gestión y protección
- Etapa 3: Respuesta a Ciberincidentes

ETAPA 1

Definición del contexto

Contexto: Ciberseguridad Empresarial

- Objeto
- Diagrama contexto
- Priorización de activos por actividad de AES
- Identificación del Marco Normativo
- Identificación de amenazas sobre los activos de valor

Contexto: Ciberseguridad Empresarial

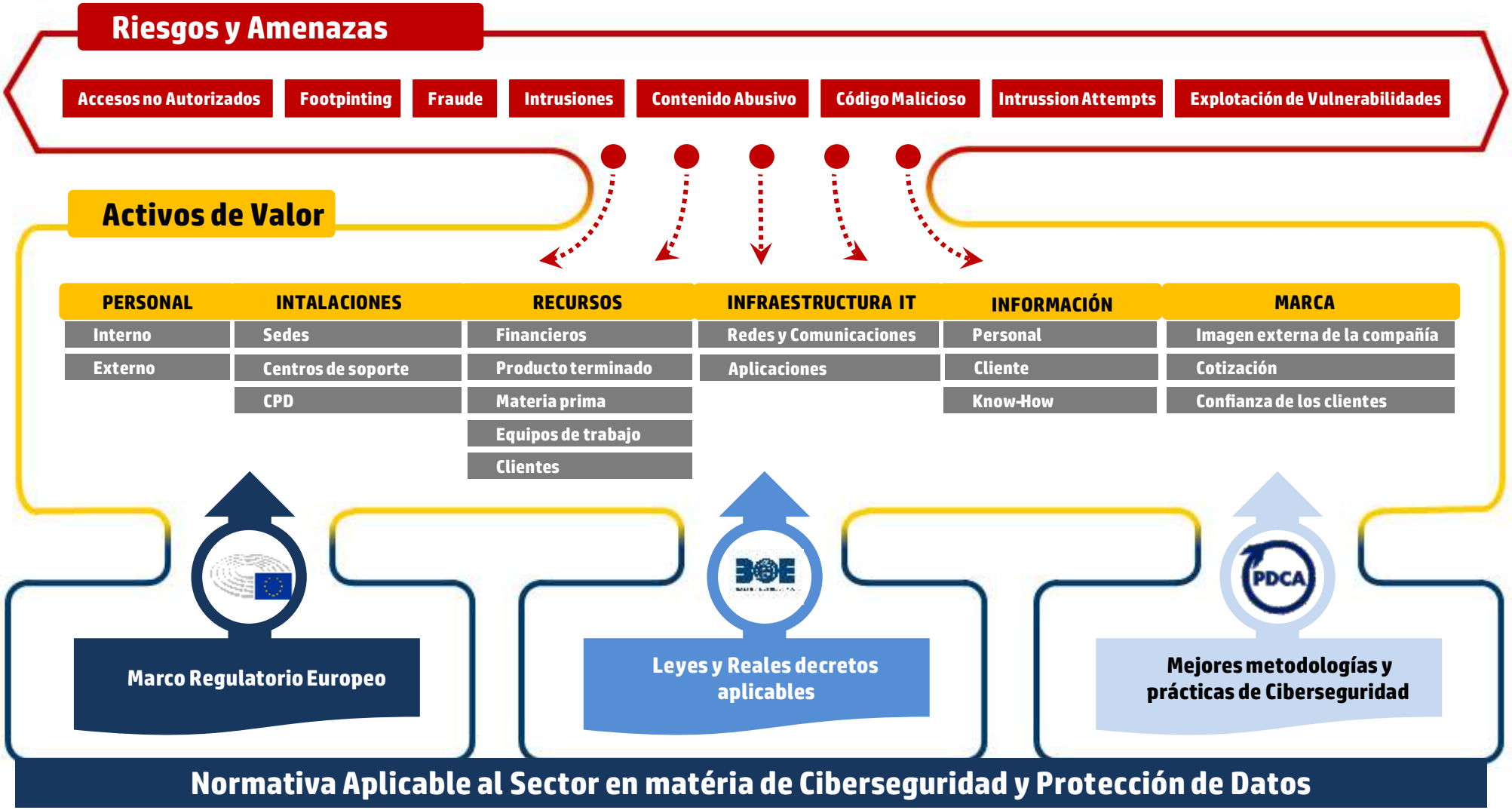
ETAPA 1: Objeto

El Objetivo de la etapa 1 o etapa de Contexto es:

- Determinar los principales Activos de Valor para las empresas del sector , catalogándolos por su criticidad en cuanto a los datos de clientes y mantenimiento del servicio .
- Identificar todo el marco normativo de obligado cumplimiento en materia de Ciberseguridad y protección de datos aplicable a las empresas del sector.
- Determinar las amenazas a las que más expuestos están o puedan estar los activos de valor, así como las más reseñadas por el marco normativo .

Contexto: Ciberseguridad Empresarial

ETAPA 1: Diagrama contexto



Contexto: Ciberseguridad Empresarial

ETAPA 1: Priorización de activos por actividad de AES

Se han considerado los siguientes grupos de activos de valor, no es una relación exhaustiva de todos los activos, se trata solo de agrupar los principales activos de valor de las empresas del sector, que tengan relación con los clientes y el mantenimiento del servicio. Además se han clasificado las actividades empresariales de AES en cuatro grupos, obteniéndose así la siguiente matriz:

		Actividades empresas AES			
		CRA	INTEGRADOR	FABRICANTE	CIBERSEGURIDAD
Activos	Marca	SECUNDARIO	SECUNDARIO	SECUNDARIO	SECUNDARIO
	Datos de carácter personal	PRINCIPAL	PRINCIPAL	SECUNDARIO	PRINCIPAL
	Comunicaciones	PRINCIPAL	PRINCIPAL	SECUNDARIO	PRINCIPAL
	Seguridad equipamiento	SECUNDARIO	SECUNDARIO	PRINCIPAL	PRINCIPAL
	Seguridad diseño	PRINCIPAL	PRINCIPAL	PRINCIPAL	PRINCIPAL
	CTV	PRINCIPAL	PRINCIPAL	SECUNDARIO	SECUNDARIO
	Datos negocio Clientes	PRINCIPAL	PRINCIPAL	SECUNDARIO	PRINCIPAL
	Datos del servicio Clientes	PRINCIPAL	PRINCIPAL	SECUNDARIO	PRINCIPAL

Tabla 1 : Matriz de priorización de Activos de valor por cada actividad Empresarial del AES

Todos los aspectos de Ciberseguridad son importantes, pero ante la necesidad de priorizar se considera que hay de dos tipos Principal y Secundario .

Contexto: Ciberseguridad Empresarial

ETAPA 1: Identificación del Marco Normativo

Marco regulatorio Europeo

- Reglamento General de Protección de Datos (RGPD)

Leyes y Reales Decretos

- Ley 5/2014, de 4 de abril, de Seguridad Privada
- Código de Seguridad Privada
- Código de Seguridad Ciudadana
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico
- Ley 59/2003, de 19 de diciembre, de firma electrónica
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Código de Protección de Datos de Carácter Personal
- Código de Derecho de la Ciberseguridad
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS)
- Real Decreto 1072/2015, de 27 de noviembre, por el que se modifica el Reglamento de la Infraestructura para la Calidad y la Seguridad Industrial
- Real Decreto -ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

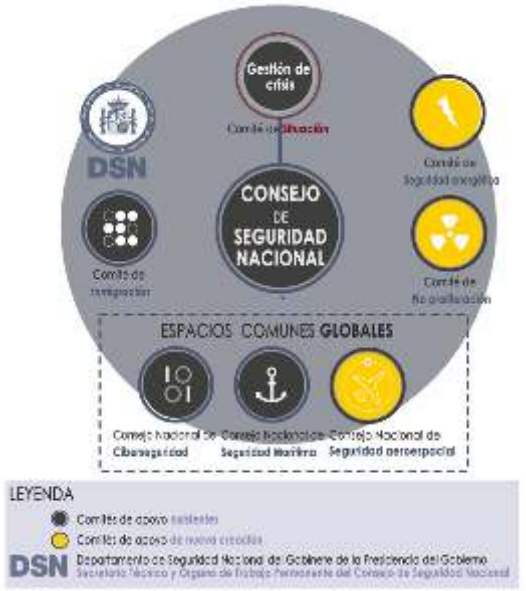
Metodologías y buenas prácticas

- ISO 27001 Gestión de la Seguridad de la Información.
- Norma ISO/IEC 15408, Common Criteria.
- Esquema Nacional de Seguridad (ENS)
- ISO 22399: Guía para la preparación ante incidentes y continuidad operacional.
- ISO 31000: Gestión de riesgos
- UNE -EN ISO 22301:2015 Gestión de la continuidad del negocio.
- BOE -A-2019-6347 Estrategia Nacional de Ciberseguridad 2019

Contexto: Ciberseguridad Empresarial

ETAPA 1: Identificación del Marco Normativo

- Unidad de Acción
- Anticipación (Prevención vs Reacción)
- Apostar más por la medidas Preventivas que por las Reactivas con la finalidad de minimizar los efectos de la amenaza
  - Eficiencia en la comunicación (protocolos, normalización, ...)
  - Aproximación al tiempo real o pseudo real
  - Minimizar el tiempo de respuesta
- Eficiencia : Sistemas Multipropósito
- Resiliencias : Asegura la disponibilidad



Contexto: Ciberseguridad Empresarial

ETAPA 1: Identificación de amenazas sobre los activos de valor

Taxonomía de amenazas

Para determinar las amenazas a las que más expuestos están o puedan estar los activos de valor, así como las más reseñadas por el marco normativo. Se decidió entre las empresas participantes utilizar la taxonomía publicada por un organismo de reconocida solvencia .

La taxonomía publicada por ENISA en las dos siguientes publicaciones fue la escogida para realizar la identificación de amenazas .

Se adjuntan como anexo

https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
https://www.enisa.europa.eu/publications/communication-network-interdependencies-in-smart-grids

Incibe ha publicado una taxonomía de amenazas que se basa en las citadas publicaciones de ENISA .

https://www.incibe-cert.es/blog/riesgos-y-retos-ciberseguridad-y-privacidad-iot

A partir de la taxonomía de ENISA se construyo una matriz de identificación cruzándola con la priorización de activos, obteniendo la "Tabla 2"

Contexto: Ciberseguridad Empresarial

ETAPA 1: Identificación de amenazas sobre los activos de valor

A partir de la información aportada:

		Activos de valor							
Categoría	**Amenaza**	**Marca**	**Datos de carácter personal**	**Comunicaciones**	**Seguridad equipamiento**	**Seguridad diseño**	**Vídeo**	**Datos negocio Clientes**	**Datos del servicio Clientes**
Ataques/Abusos	Malware								
	Secuencia de Exploit								
	Ataques dirigidos								
	DDoS								
	Falsificación de dispositivos maliciosos								
	Ataques ala privacidad								
	Modificación de Información								
	Ataques ala privacidad								
Eavesdropping/ Interception Secuestro	Man in the middle								
	Secuestro de protocolo de comunicación Iot								
	Intercepción de información								
	Reconocimiento de red								
	Secuestro de sesión								
	Obtención de información								
	Reproducción de mensajes								
Caídas	Caída de red								
	Fallos de dispositivos								
	Fallo de sistema								
	Pérdida de servicios de soporte								
Daño / Pérdida (Activos TI)	Cifrado de datos/ información confidencial								
Fallos / Averías	Vulnerabilidades del software								
	Fallos de terceros								
Ataques físicos	Modificación de dispositivos								
	Destrucción del dispositivo (sabotaje)								

Tabla 2 : Matriz de identificación de vulnerabilidades para cada activo

ETAPA 2

Medidas de gestión y protección

- Objeto
- Diagrama
- Matriz de estándares. Por actividad empresarial
- Controles de seguridad sobre los Activos de Valor
- Definiciones de Controles de seguridad

Medidas de gestión y protección

ETAPA 2: Objeto

El Objetivo de la etapa 2 es:

- Establecer una base de las **medidas de gestión y protección** sobre los **activos, sistemas y procesos** siguiendo los puntos de control que conforman los pilares de la Ciberseguridad.

  - Determinando los **controles de seguridad** a seguir para los **activos, sistemas y procesos**.

  - Seleccionar las **metodologías** y estándares para la **gestión** de la seguridad de la información.

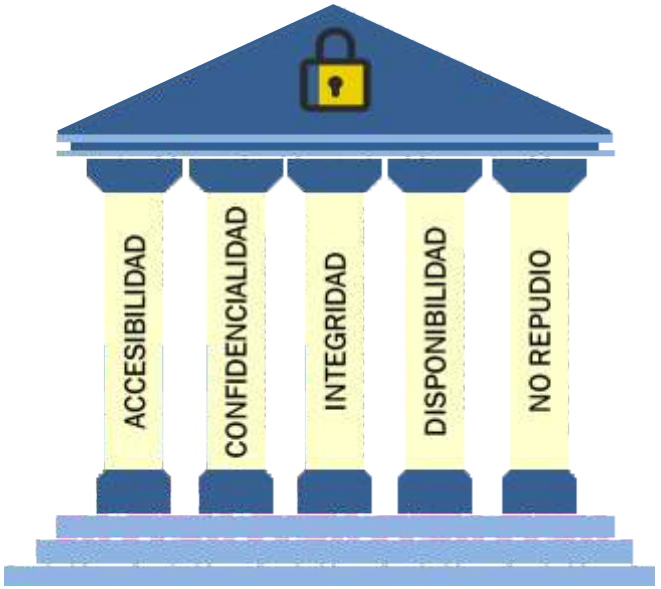
Medidas de gestión y protección

ETAPA 2: Diagrama

Gestión de los riesgos de Ciberseguridad

Establecimiento de Normativas de Protección

Gestión, Revisión, Mejora y Sostenibilidad



1. Definición de una estrategia de Ciberseguridad
2. Gestión de los riesgos de Ciberseguridad
3. Promoción de una cultura de la Ciberseguridad
4. Establecimiento de Normativas de Protección
5. Gestión, Revisión, Mejora y Sostenibilidad

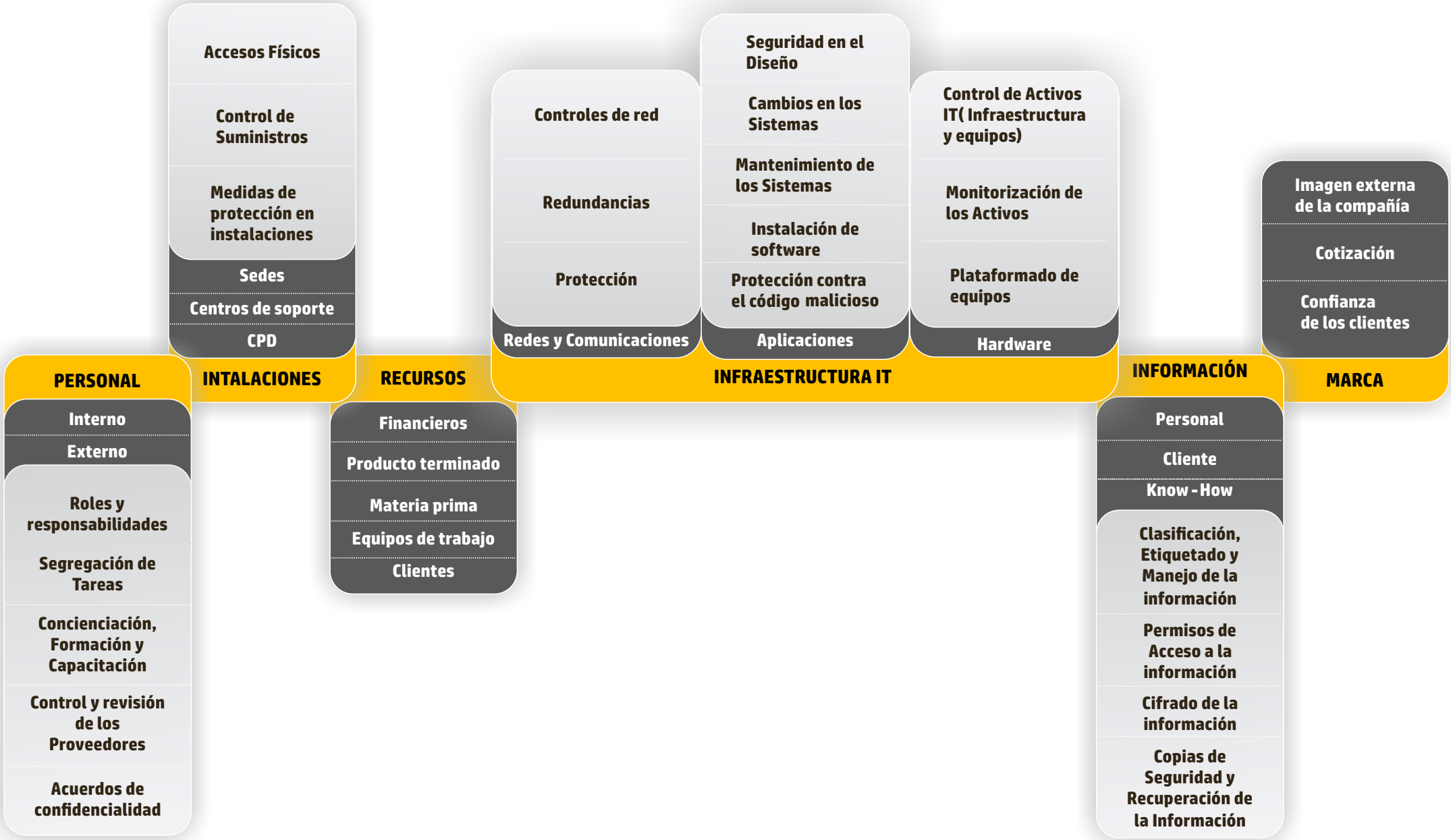
Medidas de gestión y protección

ETAPA 2: Matriz de estándares. Por actividad Empresarial

			Actividades empresas AES			
			CRA	INTEGRADOR	FABRICANTE	CIBERSEGURIDAD
Buenas Prácticas y Estándares	ISO/IEC 27001	UNE-EN ISO/IEC 27001:2017	PRINCIPAL	SECUNDARIO		PRINCIPAL
	ens	Esquema Nacional de seguridad	PRINCIPAL	SECUNDARIO		PRINCIPAL
	LEET SECURITY	Leet Security	PRINCIPAL	SECUNDARIO		PRINCIPAL
	NIST	Cibersecurity Framework by NIST	PRINCIPAL	SECUNDARIO		PRINCIPAL
	PCI	Payment Card Industry (PCI) - Software Security Framework	SECUNDARIO	SECUNDARIO	PRINCIPAL	SECUNDARIO
	PCI	Payment Card Industry (PCI) - Data Security Evaluation	PRINCIPAL	SECUNDARIO	PRINCIPAL	PRINCIPAL
	Common Criteria	Common Criteria for Information Technology Security Evaluation	SECUNDARIO	SECUNDARIO	PRINCIPAL	SECUNDARIO
	CCN	CCN-LINCE	SECUNDARIO	SECUNDARIO	PRINCIPAL	SECUNDARIO
	FIPS	FIPS (Federal Information Processing Standard)	SECUNDARIO	SECUNDARIO	PRINCIPAL	SECUNDARIO

Medidas de gestión y protección

ETAPA 2: Controles de seguridad sobre los Activos de Valor



Medidas de gestión y protección

ETAPA 2: Definiciones de Controles de seguridad

Personas	Roles y responsabilidades	Se debe contar con roles específicos para el desempeño de las funciones en materia de seguridad de la información y continuidad de negocio. Las responsabilidades de estos roles deben ser claras e identificables con puestos específicos.
	Segregación de Tareas	Se debe optar por políticas de "información mínima Disponible; es decir que las distintas líneas operativas; así como la parte de gestión y administrativa no tenga acceso a la misma información a no ser que sea estrictamente necesario.
	Concienciación, Formación y Capacitación	Todo el personal y especialmente las personas que manejan información sensible, deben de ser consciente de los riesgo derivados de su actividad y los sistemas así como estar formados y capacitados en prácticas seguras que minimicen o eliminen los riesgos de su actividad.
	Control y revisión de los Proveedores	Los proveedores que sean críticos para la información así como para las actividades del negocio deben controlarse mediante Acuerdos a nivel de servicio, verificar el cumplimiento de dichos acuerdos y realizar evaluaciones periódicas de dichos proveedores.
	Acuerdos de confidencialidad	Los proveedores que tengan acceso a Información relevante para la empresa deberán firmar acuerdos de confidencialidad para proveer el servicio.
Información	Clasificación, Etiquetado y Manejo de la información.	La información Recopilada, generada procesada por la entidad deberá ser catalogada en función de su criticidad y etiquetada en consecuencia. Además se deberán de establecer normas y protocolos para tratar las categorías más relevantes de información.
	Permisos de acceso a la Información	Se debe optar por políticas de "información mínima Disponible"; es decir que las distintas líneas operativas; así como la parte de gestión y administrativa no tenga acceso a la misma información a no ser que sea estrictamente necesario.
	Cifrado de la Información	La información más critica deberá encontrarse cifrada para evitar fugas o robos de información.
	Copias de Seguridad y Recuperación de la información.	Los soportes con información más critica deberán contar con copias de seguridad disponible y establecer protocolos de recuperación para dicha información.
Hardware	Control de Activos IT (Infraestructura)	Contar con un Inventario actualizado donde se reflejen los distintos activos y los propietarios.
	Control de Activos IT (Equipos)	Controlar las adquisiciones y devoluciones de los equipos de trabajo.
	Monitorización de los activos.	Los activos con información sensible deberán estar monitorizados para controlar las personas que acceden.
	Plataforma de equipos.	Los equipos de los distintos usuarios deberán plataformarse con el software aprobado por la compañía, el sistema de antivirus y el cifrado de disco duro que recomienda la compañía.
Software	Seguridad en Diseño	Los desarrollos propios o subcontratados deberán integrar los criterios de seguridad desde el diseño.
	Cabios en los sistemas	Los cambios en los sistemas deberán ser aprobados y realizar pruebas de seguridad y funcionalidad en entornos seguros separados del entorno de producción.
	Mantenimiento de los Sistemas	Se deberán identificar las vulnerabilidades de los sistemas y solventarlas, así como mantener actualizadas las versiones y parches de seguridad para los distintos sistemas.
	Instalación de Software	La instalación de Software en los equipos debe estar controlada, pasando por un proceso de aprobación para cada tipo de software que desee instalarse en los equipos.
	Protección contra el código Malicioso.	Se deberá contar con medidas de detección, prevención y recuperación contra el código malicioso, tanto en equipos como en la infraestructura IT.
Redes	Controles de red	Las redes deberán ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones, Identificando los mecanismos de seguridad, niveles de servicio de red y requisitos de gestión. Esta información deberá incluirse en los acuerdos para el mantenimiento de red ya sea de forma interna o externa.
	Redundancias.	Se deberá contar con redes de respaldo seguras para cuando la red principal no este disponible.
	Protección del trafico de red	Las redes deberán contar con elementos de protección para el acceso a la red y a los sistemas así como monitorizar y protegerel trafico de red
Emplazamientos	Accesos Físicos	Los accesos físicos a las instalaciones y a zonas especificas de instalaciones deben contar con elementos de control de acceso para protegerse de los accesos indebidos.
	Control de Suministros	Las instalaciones deberán contar con sistemas que aseguren la continuidad del suministro eléctrico frente a corte puntuales.
	Medidas de protección en instalaciones	Las instalaciones deberán contar con los sistemas de prevención, detección, alerta y actuación necesarios para proteger a las personas, activos e información de las instalaciones, frente a eventos disruptivos que alteren las operaciones y la seguridad del negocio.

ETAPA 3

Respuesta a ciberincidentes

- Objeto
- Taxonomía de ciberincidentes
- Criterios de Nivel de Peligrosidad
- Nivel de impacto
- Fases para la gestión de un ciberincidente
- Diagrama ciclo de vida de un ciberincidente

Respuesta a ciberincidentes

ETAPA 3: Objeto

El Objetivo de la etapa 3 es:

- Determinar los mecanismos mínimos con los que deban contar las empresas del sector para dar respuesta a ciberincidentes.
  - Identificando el contexto del ciclo de vida de un ciberincidente.
  - Determinando las herramientas y medios necesarios con los que se debe de contar para actuar en cada fase del ciclo de vida.
  - Seleccionar las metodologías, estándares e indicadores necesarios para evidenciar que se cuenta con todos estos mecanismos.

Respuesta a ciberincidentes

ETAPA 3: Taxonomía de ciberincidentes

Contenido abusivo	Spam
Contenido dañino	Sistema infectado
	Servidor C&C (Mando y Control)
	Distribución malware
	Configuración malware
	Malware dominio DGA
Obtención de información	Escaneo de redes (scanning)
	Análisis de paquetes (sniffing)
	Ingeniería social
Intento de intrusión	Explotación de vulnerabilidades conocidas
	Intento de acceso con vulneración de credenciales
	Ataque desconocido
Intrusión	Compromiso de cuenta con privilegios
	Compromiso de cuenta sin privilegios
	Compromiso de aplicaciones
	Robo
Disponibilidad	DoS
	DDoS
	Sabotaje
	Interrupciones
Compromiso de la información	Acceso no autorizado a información
	Modificación no autorizada de información
	Pérdida de datos
Fraude	Uso no autorizado de recursos
	Derechos de autor
	Suplantación
	Phishing
Vulnerabilidades	Criptografía débil
	Amplificador DDoS
	Servicios con acceso potencial no deseado
	Revelación de información
	Sistema vulnerable
Otros	Otros
	APT
	Daños informáticos

Asociación Española de empresas de Seguridad

Respuesta a ciberincidentes

ETAPA 3: Criterios de nivel de Peligrosidad

CRÍTICO	Otros	• APT • Daños informáticos
MUY ALTO	Código dañino	• Distribución de malware • Configuración de malware
	Intento de intrusión	• Ataque desconocido
	Intrusión	• Robo
	Disponibilidad	• Sabotaje • Interrupciones
ALTO	Código dañino	• Sistema infectado
	Código dañino Intento de intrusión	• Servidor C&C • Malware Dominio DGA • Compromiso de aplicaciones
	Disponibilidad	• DoS • DDoS
	Compromiso de la información	• Acceso no autorizado a información • Modificación no autorizada de información • Pérdida de datos
	Fraude Phishing	• Fraude Phishing
MEDIO	Obtención de información	• Ingeniería social
	Intento de intrusión	• Explotación de vulnerabilidades conocidas • Intento de acceso con vulneración de credenciales
	Intrusión	• Compromiso de cuentas con privilegos
	Fraude	• Uso no autorizado de recursos • Derechos de autor • Suplantación
	Vulnerable	• Criptografía débil • Amplificador DDoS • Servicios con acceso potencial no deseado • Revelación de información • Sistema vulnerable
BAJO	Contenido abusivo	• Spam
	Obtención de información	• Escaneo de redes (scanning) • Análisis de paquetes (sniffing)
	Intrusión	• Compromiso de cuentas sin privilegios
	Otros	• Otros

Respuesta a ciberincidentes

ETAPA 3: Nivel de impacto

CRÍTICO	• Afecta a más del 90% de los sistemas de la empresa • Interrupción en la prestación del servicio superior a 24 horas y superior al 50% de los usuarios. • El ciberincidente precisa para resolverse más de 30 Jornadas -Persona. • Impacto económico superior al 3 % de la facturación • Extensión geográfica nacional. • Daños reputacionales muy elevados y cobertura continua en medios de comunicación
MUY ALTO	• Afecta a más del 75% de los sistemas de la organización. • Interrupción en la prestación del servicio superior a 8 horas y superior al 35% de los usuarios. • El ciberincidente precisa para resolverse entre 10 y 30 Jornadas -Persona. • Impacto económico entre el 1 % y el 3 % de la facturación. • Extensión geográfica superior a 4 CC.AA. • Daños reputacionales elevados y cobertura continua en medios de comunicación
ALTO	• Afecta a más del 50% de los sistemas de la organización. • Interrupción en la prestación del servicio superior a 1 hora y superior al 10% de usuarios. • El ciberincidente precisa para resolverse entre 5 y 10 Jornadas –Persona. • Impacto económico entre el 1 % y el 0,5 % de la facturación. • Extensión geográfica superior a 3 CC.AA. • Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
MEDIO	• Afecta a más del 20% de los sistemas de la organización. • Interrupción en la presentación del servicio superior al 5% de usuarios. • El ciberincidente precisa para resolverse entre 1 y 5 Jornadas -Persona. • Impacto económico entre el 0,5 % y el 0,1 % de la facturación. • Extensión geográfica superior a 2 CC.AA. • Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).
BAJO	• Afecta a los sistemas de la organización. • Interrupción de la prestación de un servicio. • El ciberincidente precisa para resolverse de menos de 1 jornada - persona. • Impacto económico entre el 0,1 % y el 0,05 % de la facturación. • Daños reputacionales puntuales, sin eco mediático.
SIN IMPACTO	• No hay ningún impacto apreciable.

Respuesta a ciberincidentes

ETAPA 3: Fases para la gestión de un ciberdelincuente

PREPARACIÓN

- Disponer de información actualizada de contacto.
- Mantener las políticas y procedimientos actualizados.
- Herramientas a utilizar en todas las fases de gestión de un ciberincidente.
- Formación del equipo humano para mejorar las capacidades técnicas y operativas.
- Realizar análisis de riesgos que permita disponer de un plan de tratamiento de riesgos.
- Ejecución de ciberejercicios a fin de entrenar las capacidades y procedimientos técnicos, operativos, de gestión y coordinación.

IDENTIFICACIÓN

- Registrar y monitorizar los eventos de las redes, sistemas y aplicaciones.
- Recolectar información situacional que permita detectar anomalías.
- Disponer de capacidades para descubrir ciberincidentes y comunicarlos a los contactos apropiados.
- Recopilar y almacenar de forma segura todas las evidencias.
- Compartir información con otros equipos internos y externos de forma bidireccional para mejorar las capacidades de detección.

CONTENCIÓN

- Registrar y monitorizar los eventos de las redes, sistemas y aplicaciones.
- Recolectar información situacional que permita detectar anomalías.
- Disponer de capacidades para descubrir ciberincidentes y comunicarlos a los contactos apropiados.
- Recopilar y almacenar de forma segura todas las evidencias.
- Compartir información con otros equipos internos y externos de forma bidireccional para mejorar las capacidades de detección.

MITIGACIÓN

- Determinar las causas y los síntomas del ciberincidente para determinar las medidas de mitigación más eficaces.
- Identificar y eliminar todo el software utilizado por los atacantes.
- Recuperación de la última copia de seguridad limpia.
- Identificar servicios utilizados durante el ataque.

RECUPERACIÓN

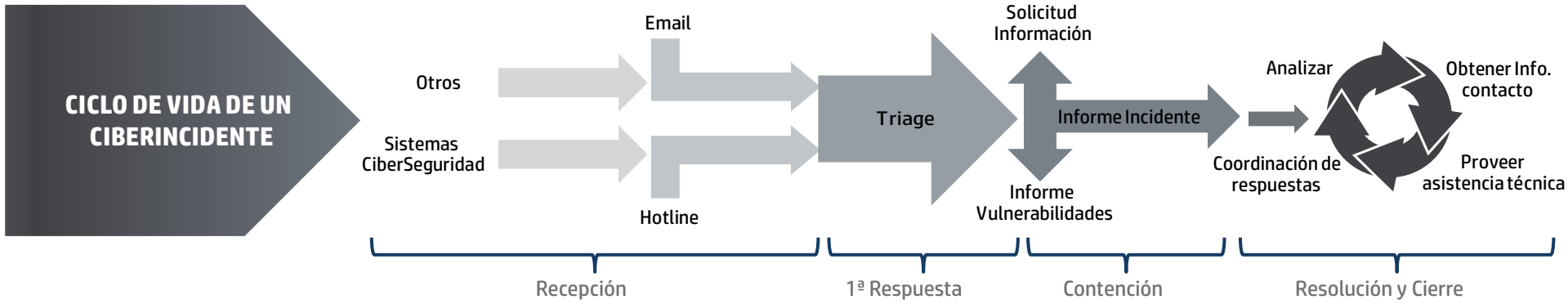
- Conviene prestar especial atención a estos sistemas durante la puesta en producción y buscar cualquier signo de actividad sospechosa, definiendo un periodo de tiempo con medidas adicionales de monitorización.

POST-INCIDENTE

- Reflexionar sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciberincidente y todos los problemas asociados a la misma.
- Aprender de lo sucedido y tomar las medidas adecuadas para evitar que una situación similar se pueda volver a repetir.
- Informe del ciberincidente.

Respuesta a ciberincidentes

ETAPA 3: Diagrama ciclo de vida de un ciberincidente



ASPECTOS A TENER EN CUENTA PARA LA GESTIÓN DE CIBERINCIDENTES

Inventario Documental para la gestión de Incidentes

- Procesos Operativos de Seguridad
- Plan de Continuidad del Negocio
- Plan de Recuperación ante Desastres

Contactos internos en caso de emergencia

- Directorios de responsables de Áreas
- Equipos de Respuesta internos con los que cuenta la Compañía
- Centros alternativos

Contactos Externos en caso de emergencia

- Organismos Oficiales y Asociaciones
- Fabricantes y Proveedores Relevantes

Elementos de comunicación

- Herramientas Para la gestión de incidentes
- Sistemas de escalado, herramientas de tiketing, cascada de teléfonos, etc.
- Cuentas Oficiales en las RRSS de la Compañía.

HITOS 2020

Asociación Española de empresas de Seguridad

Hitos 2020

Taxonomizar los activos IT de las empresas	■ Realizar análisis de los distintos tipos de activos IT con los que cuentan las empresas del sector diferenciando por actividad (integradores, CRA, Ciberseguridad, Fabricantes) ■ Seleccionar una taxonomía propuesta por un organismo de referencia en Ciberseguridad.
Establecer niveles de categorización de la información comunes	■ Identificar todos los tipos de información con las que cuentan las empresas del sector diferenciando por actividad (integradores, CRA, Ciberseguridad, Fabricantes). ■ Seleccionar la categoría dictada por los organismos del estado en materia RGPD. ■ Establecer un marco de categorización de la información.
Establecer una metodología de riesgos común	■ Es preciso contar con una taxonomía de riesgos y amenazas (ya establecida en 2019). ■ Taxonomía de activos IT y categorización de la información (a desarrollar en 2020). ■ Con estas dos premisas elegir una metodología ágil y sencilla para empezar a madurarla.
Determinar los elementos mínimos para la correcta gestión de incidentes	■ Identificar los planes, procesos y protocolos mínimos necesarios más adecuados para las empresas del sector. ■ Identificar las salvaguardas y elementos de monitorización y alerta temprana más recomendada para las empresas del sector. ■ Seleccionar una lista de servicios para la contención y remediación de ciberincidentes con los que deben contar las distintas empresas, ya sean de forma interna o externalizada.

Asociación Española de Empresas de Seguridad
C/Alcalá, 99 2ºA - 28009 Madrid
Telf. 915 765 225
www.aesseguridad.es - aes@aesseguridad.es
@aes_seguridad