*[Adecuación al Esquema Nacional de Seguridad: Un Enfoque Integral]

Autor: Vanesa Gil Laredo
Responsable Consultoría S21Sec
CISA, CISM, CGEIT, Lead Auditor, QSA
Presenta : Roberto Martin Gerente AAPP
Tfno 660981379 ; rmartin@s21sec.com

S21sec
Unidad de Servicios Globales de Seguridad

ÍNDICE

Quienes somos

Empresa especializada en servicios de seguridad de la información:

- Líder y referente en el sector de la seguridad digital.
- Fundada en el año 2000 con la vocación de prevenir y gestionar el riesgo de las organizaciones y las personas en su vida digital.
- Vocación de contribuir a la creación de una verdadera cultura de la seguridad en las organizaciones.
- 200 técnicos especialistas en seguridad
- Primer CERT / SOC en España

S21sec está dedicada en exclusiva a la Seguridad de la Información

S21Sec, Servicios de Seguridad Informática

- 8 oficinas en España
- 3 oficinas internacionales
- 2 partners internacionales

Nuestra diferencia:

✓El mayor equipo de especialistas en seguridad digital en España: 265 Empleados
✓La innovación como motor de negocio.
✓Primer centro de I+D+i de seguridad en Europa
✓La apuesta por la calidad y las certificaciones como proceso esencial
✓Una protección y prevención ante incidentes 24x7x365
✓Una plataforma de gestión integral

Nuestras unidades de negocio

S21sec UMSS
Unidad de Servicios Globales de Seguridad

- Consultoría estratégica
- Servicios 24x7: Compliance, gestión de dispositivos, evaluación seguridad, formación y concienciación

S21sec e-crime
Unidad de Inteligencia

- Fraude
- Vigilancia Digital
- Inteligencia

S21sec tech
Unidad de Productos

bitacora

S21sec university
Unidad de Formación

- Formación especializada
- Planes de carrera
- Cursos Online

S21sec labs
Unidad de I+D+i

- Proyectos a medida
- Evaluación y análisis de tecnologías
- Consultoría de I+D+i

S21sec

S21sec labs : Líneas de investigación

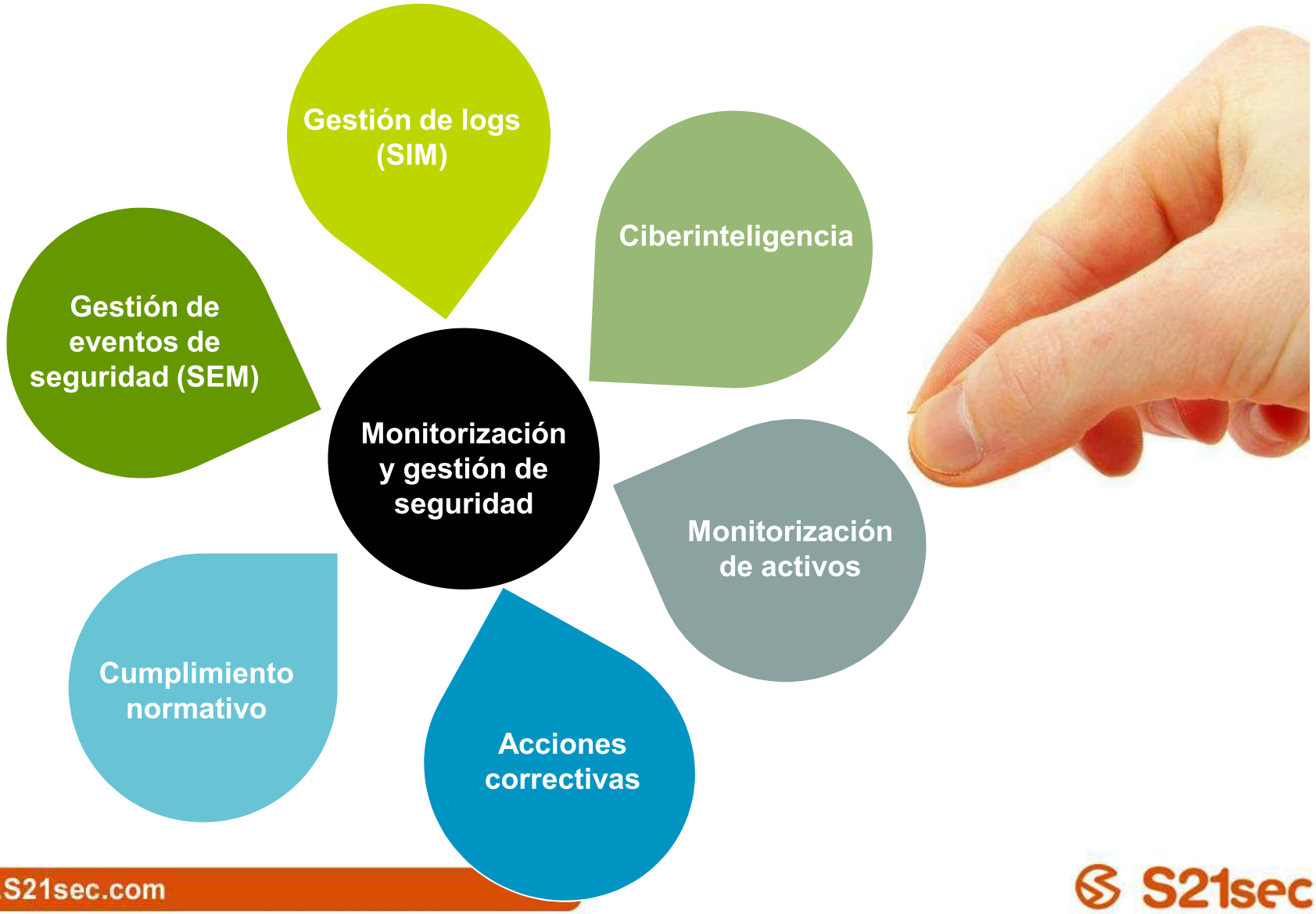
S21sec labs
Unidad de I+D+i

Proyectos a medida

Evaluación y análisis de tecnologías

Investigación y desarrollo

Soluciones: Suite Bitacora v5



S21sec

Bitacora Horizon

- Es una plataforma de gestión centralizada de todos los activos informáticos de su organización, que permite administrar la seguridad de los puestos de trabajo.

Bitacora Horizon ofrece una consola de administración y un sistema de agentes distribuido que permiten realizar cualquier acción, desde un único punto central de forma eficaz y eficiente 3n cualquier puesto o servidor esté donde esté

El mayor equipo en España de Seguridad Digital: 200 especialistas

CISA · CISSP · OSSTMM · CISM · GCIA · GSEC

Microsoft Certified Partner | Security Solutions

SEIPartner

Un modelo de Gestión integral de la Seguridad 24 horas. CIS

NUESTRA DIFERENCIA

Desde los inicios, apostando por la innovación y el desarrollo de soluciones de vanguardia.
Primer centro I+D+i de Europa

S21sec labs
La seguridad digital del futuro, hoy

PCI Security Standards Council — APPROVED SCANNING VENDOR

PCI Security Standards Council — QUALIFIED SECURITY ASSESSOR

IQNet · AENOR ER Empresa Registrada UNE-EN ISO 9001 · AENOR ER Gestión I+D+i UNE 166002 · AENOR ER Capacidad Software 1 ISO/IEC 15504 · AENOR ER Seguridad Información UNE-ISO/IEC 27001

Y siempre, calidad y certificaciones

Esquema Nacional de Seguridad (ENS)

- El Real Decreto 3/2010, de 8 de enero, regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, de obligado cumplimiento para las Administraciones Públicas.

- Desarrollado en base a lo establecido en el artículo 42.2 de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.

- Objetivo: *"La creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios"*.

- Si hubiera circunstancias que impidan la plena aplicación de lo exigido en el ENS, se deberá definir un Plan de Adecuación que establezca los plazos de ejecución, no pudiendo ser estos superiores a 48 meses.

Donde deberíamos estar?

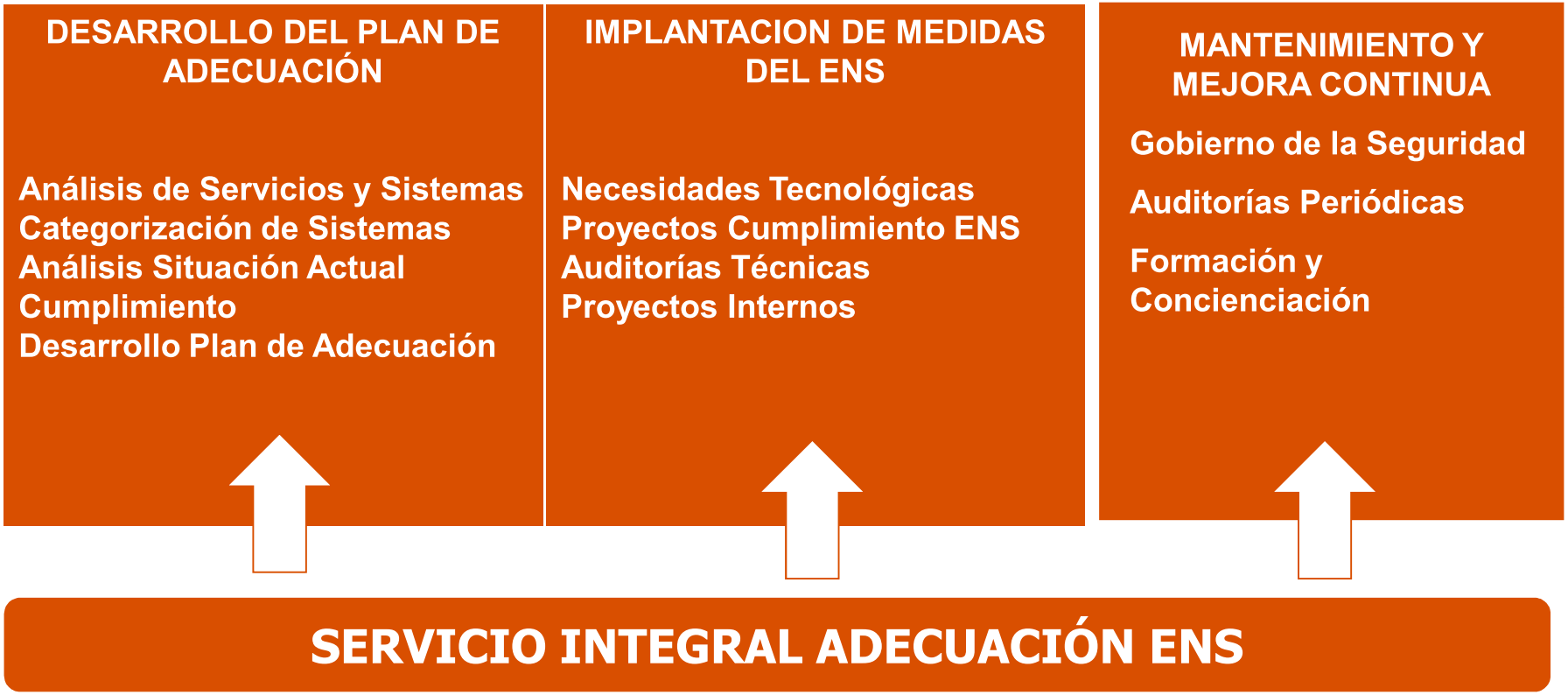
- Fecha objetivo:
  - 31 ·Enero 2011 Adecuación al ENS (Mínimo contar con un plan de adecuación)
  - 31 de Enero 2014 Finalizada la adecuación

- **La realidad: Es muy diversa**
- **Que deberíamos hacer?**
  - **Deberíamos intentar contar con un plan de adecuación**

Y Cuando ya hemos asegurado el cumplimiento?

- Implementar las medidas del Plan de mejora de la seguridad
- Evaluar las medidas adoptadas fruto de nuestro plan de adecuación
- Mantener el sistema actualizado
- Realizar una auditoria de seguridad

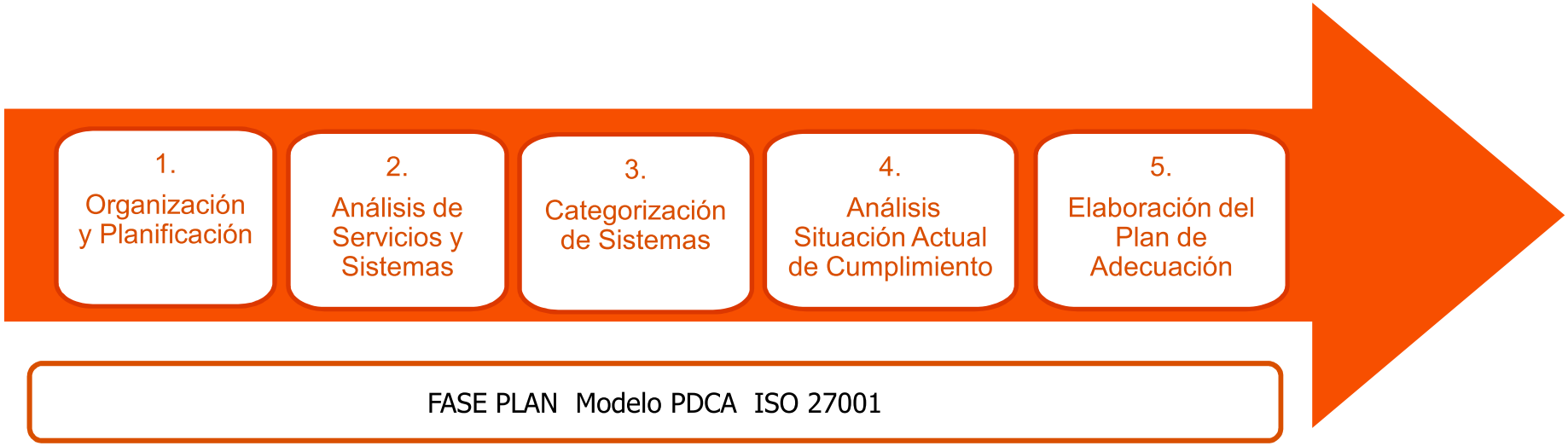
Servicio Integral Adecuación ENS



S21sec

Plan de Adecuación ENS

La metodología empleada para el desarrollo del Plan de Adecuación al ENS es la que se detalla a continuación:



S21sec

Fases previas

- **Análisis de Servicios y Sistemas.**
  - Analizar los servicios de la organización incluidos en el alcance del ENS, identificando los sistemas que soportan dichos servicios y la información asociada a los mismos.
  - Documentación del alcance del ENS, detallando los servicios y sistemas incluidos en el ámbito del ENS.

- **Categorización de los Sistemas.**
  - Categorización de los sistemas en base a los criterios definidos por el ENS.
  - Determinación de las dimensiones de seguridad relevantes: Confidencialidad, disponibilidad, integridad, autenticidad, trazabilidad.
  - Evaluación del impacto (Bajo, Medio, Alto) para cada sistema en función de cada una de las dimensiones de seguridad:
    1. Alcanzar sus objetivos.
    2. Proteger los activos a su cargo.
    3. Cumplir las obligaciones de servicio.
    4. Respetar la legalidad vigente.
    5. Respetar los derechos de las personas.
  - Categorización de cada sistema en función del impacto en las dimensiones de seguridad: Básico, Medio, Alto.

Fases previas

- **Análisis de la Situación Actual de Cumplimiento.**
  - En función de la categoría del sistema establecida durante la fase anterior, se determinan las medidas del ENS que resultan aplicables.
  - Realización de un diagnóstico de situación actual de cumplimiento del ENS.
  - Desarrollo del Informe de Análisis de Situación Actual de Cumplimiento del ENS.
- **Desarrollo del Plan de Adecuación.**
  - Desarrollo del Plan de Adecuación en el que se establezcan las medidas a adoptar para garantizar la adecuación al ENS. El Plan contemplará todos los aspectos exigidos en la Guía de Seguridad CCN-STIC 806:
    1. Política de Seguridad
    2. Información que se maneja, con su valoración.
    3. Servicios que se prestan, con su valoración.
    4. Datos de carácter personal.
    5. Categoría del sistema o sistemas.
    6. Declaración de aplicabilidad de las medidas del Anexo II del RD 3/2010,
    7. Análisis de riesgos.
    8. Insuficiencias del sistema.
    9. Plan de mejora de seguridad.

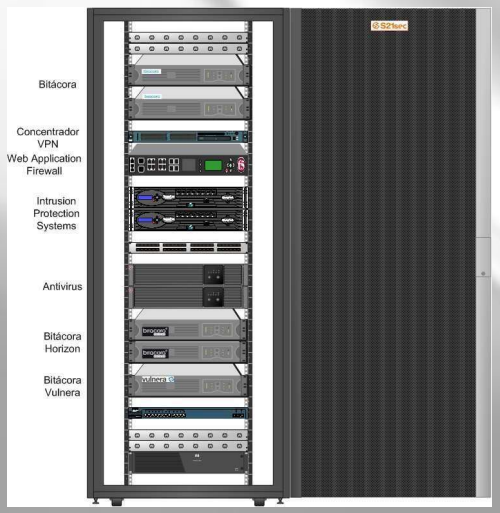
Plan de adecuacion dentro de un Servicio Integral Adecuación ENS

- Servicio Integral de Adecuación al ENS:
  - Fase 1: Elaboración de un Plan de Adecuación con fecha 30 de enero de 2011, en base a lo establecido en la Disposición Transitoria del Real Decreto 3/2010, *"Adecuación de Sistemas".*
  - Fase 2: Ejecución del Plan de Adecuación en un plazo no superior a 36 meses, en base a lo establecido en la Disposición Transitoria.
  - Fase 3: Mantenimiento y Mejora Continua.
- El proyecto de adecuación al ENS tiene como objeto la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI) que satisfaga los requisitos establecidos en el ENS, empleando como base el marco metodológico establecido en la Norma ISO 27001.
- Para el desarrollo del Plan de Adecuación y la posterior implantación de los proyectos que lo constituyen son consideradas las Guías del Centro Criptológico Nacional (CCN-STIC).

Plan de Adecuación ENS

Implantación ENS
1. Solución integral S21sec

- Solución de Monitorización y Gestión de Eventos de Seguridad
- Solución de IDS/IPS
- Software Antivirus
- Solución de Monitorización de Políticas y Seguridad de Servidores
- Solución de Cifrado de Datos



S21sec
La seguridad digital del futuro, hoy

Plan de Adecuación

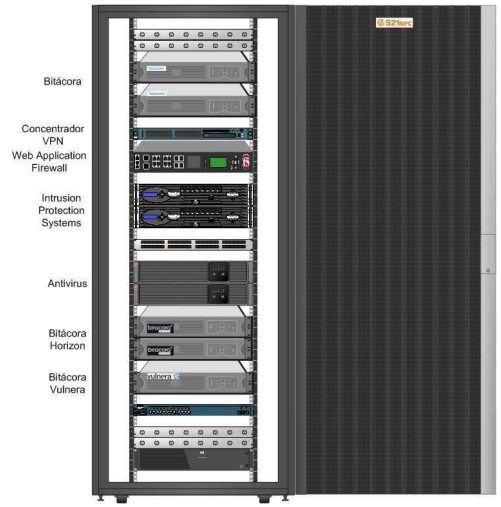
- Ejemplo

Id	Descripción	Insuficiencias Asociadas	Prioridad
PROENS01	DEFINICIÓN Y APROBACIÓN DE POLÍTICA Y NORMATIVAS DE SEGURIDAD	INS001;INS002;INS018;INS026;INS027;INS032	Alta
PROENS02	PROCEDIMIENTOS DE SEGURIDAD	INS03;INS04;INS07 INS014;INS015;INS016;INS030;INS031;INS033;INS034	Alta
PROENS03	ANÁLISIS DE RIESGOS	INS05; INS06	Alta
PROENS04	MEJORA DE CONTROL DE ACCESO LÓGICO	INS008; INS010; INS011; INS012; INS013; INS028	Media
PROENS05	DEINICIÓN Y SEGREGACIÓN DE FUNCIONES DEL PERSONAL	INS009; INS022	Media
PROENS06	CIFRADO DE ALMACENAMIENTO Y TRANSMISION	INS017	Media
PROENS07	INDICADORES DE CONTROL DE SERVICIOS EXTERNOS	INS019	Baja
PROENS08	MEJORAS EN INSTALACIONES E INFRAESTRUCTURAS	INS020; INS021	Baja
PROENS09	ACTUALIZACIÓN DE DOCUMENTO DE SEGURIDAD Y ADECUACIÓN A REGLAMENTODE DESARROLLO 1720/2007 DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL	INS037	Alta
PROENS10	PLAN DE FORMACIÓN Y CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN	INS023; INS024; INS025	Alta
PROENS11	PROTECCIÓN DE DISPOSITIVOS PORTÁTILES	INS029	Media
PROENS12	REGISTRO DE PRUEBAS DE SEGURIDAD EN DESARROLLO DE APLICACIONES	INS035; INS036	Media
PROENS13	PRUEBAS Y/O SIMULACROS DE COPIAS DE RESPALDO	INS040	Media

Asesoramiento Implantación Esquema Nacional Seguridad

Implantación ENS
1. Necesidades Tecnológicas

- Solución de Monitorización y Gestión de Eventos de Seguridad
- Solución de IDS/IPS
- Software Antivirus
- Solución de Monitorización de Políticas y Seguridad de Servidores
- Solución de Cifrado de Datos



Implantación ENS
1. Necesidades Tecnológicas

Monitorización de eventos de los diferentes dispositivos de la red del cliente.

Gestión remota desde el Security Operation Center (SOC-CERT) de S21sec en Madrid de los dispositivos de seguridad: IDS, firewalls, consola de antivirus, Horizon,… (Mantenimiento, actualizaciones periódicas, actuación frente incidentes y bajo demanda, informes periódicos,…)

Implantación ENS
2. Proyectos para Cumplimiento ENS

- Desarrollo del Cuerpo Normativo
- Consultoría de Securización de Arquitectura de Red
- Guías de Securización de Sistemas
- Metodología de Programación Segura
- Estructura Organizativa de Seguridad
- Análisis de Riesgos
- Plan de Continuidad de Negocio
- Formación y Concienciación
- Oficina Técnica ENS

Implantación ENS
3. Auditorías Técnicas

- Auditoría Bienal ENS
- Análisis de Vulnerabilidades
- Test de Intrusión
- Auditorías de Código de Aplicaciones

Implantación ENS
4. Proyectos Internos

- **Implantación de Medidas de Seguridad ENS.**
  1. Implantación de medidas de control de acceso lógico.
  2. Implantación de medidas de control de acceso físico.
  3. Implantación de Guías de Securización de Sistemas.
  4. Implantación de medidas de desarrollo seguro de software.
  5. Implantación de normativas y procedimientos de seguridad
  6. Implantación de recomendaciones de auditorías periódicas.
  7. Otros

- **Mantenimiento de Logs de Sistemas (Registros de Auditoría).**
- **Segmentación y Securización de Arquitectura de Red.**
- **Implantación del Plan de Continuidad de Negocio.**

Mantenimiento y Mejora Continua

S21sec

La seguridad digital del futuro, hoy

Cuadro de Mandos: Bitacora ENS

- Bitacora constituye una herramienta eficaz para ayudar al cumplimiento del ENS.
- Establecimiento de un cuadro de mandos que permite revisar y controlar, a través de los eventos monitorizados, el cumplimiento de:
  - Esquema Nacional de Seguridad.
  - Estándar PCI DSS
  - ISO 27001, ISO 27002,…
  - Legislación vigente de protección de datos de carácter personal (LOPD, RLOPD).
- Herramienta de gestión de logs de los sistemas incluidos en el alcance del ENS (host, firewalls, routers, servidores, bases de datos, aplicaciones,…).
- Permite disponer de indicadores, alertas y cuadros de mando en relación al cumplimiento, entre otras, de las siguientes medidas de seguridad establecidas por el ENS:
  - Control de Acceso Lógico (requisitos de acceso, mecanismos de autenticación, acceso local, acceso remoto…)
  - Protección frente a Código Malicioso.
  - Gestión de Incidencias.
  - Protección de las Comunicaciones.
  - Registro de Accesos.
  - Monitorización del sistema: Detección de Intrusión.
  - Inventario de Activos.

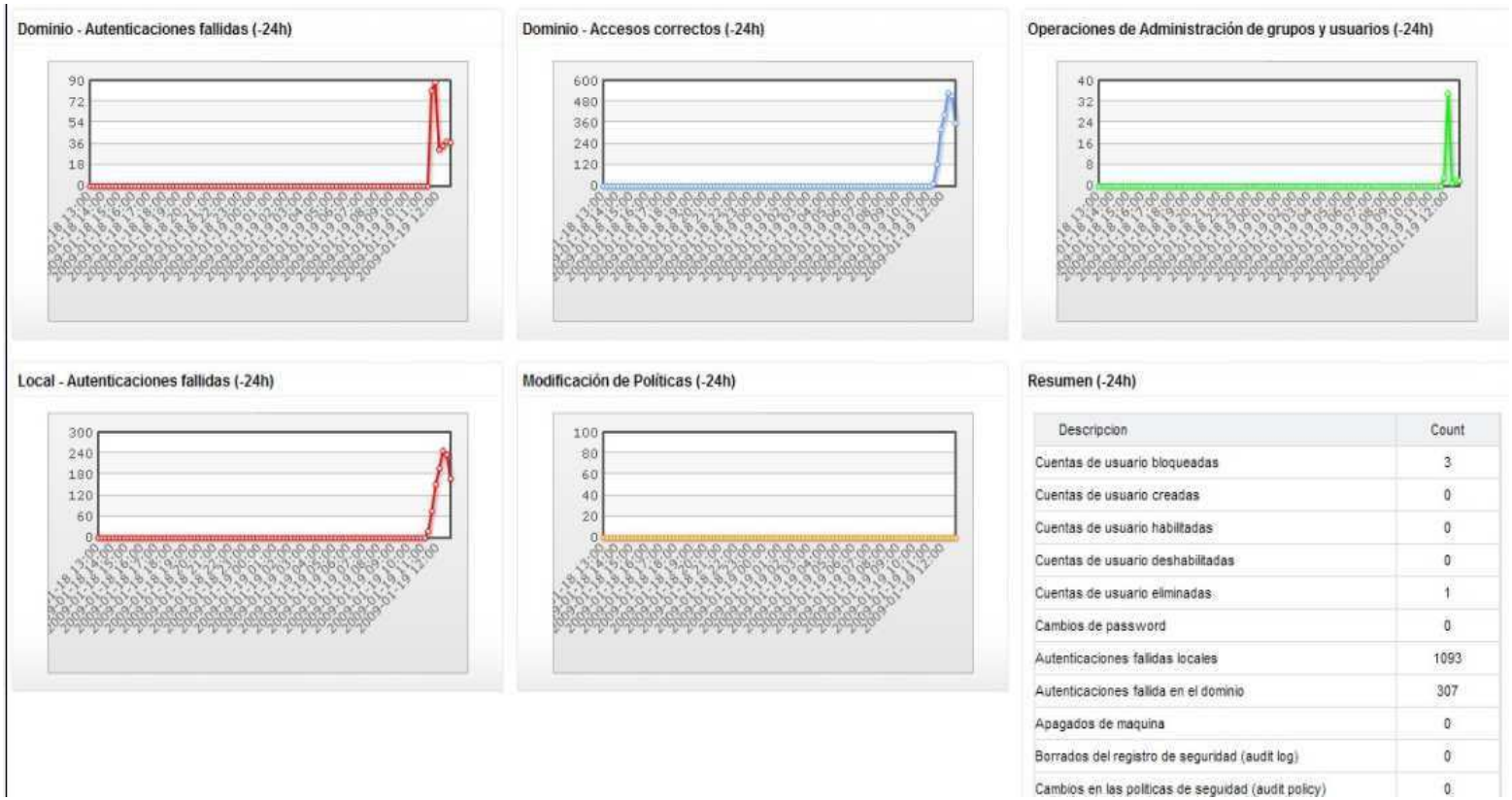
Cuadro de Mandos: Bitacora ENS

- **Monitorización de Sistemas, Bases de Datos y Aplicaciones**

S21sec

Cuadro de Mandos: Bitacora ENS

Control de Acceso Lógico



Descripcion	Count
Cuentas de usuario bloqueadas	3
Cuentas de usuario creadas	0
Cuentas de usuario habilitadas	0
Cuentas de usuario deshabilitadas	0
Cuentas de usuario eliminadas	1
Cambios de password	0
Autenticaciones fallidas locales	1093
Autenticaciones fallida en el dominio	307
Apagados de maquina	0
Borrados del registro de seguridad (audit log)	0
Cambios en las politicas de seguidad (audit policy)	0

*[MUCHAS GRACIAS]

Contacto: vgil@s21sec.com

S21sec UMSS

www.s21sec.com
info@s21sec.com
+34 902 222 521