Quien es Jordi Vidal?

- **Grado en Ingeniería Informática** en la FIB – UPC
- **Master Interuniversitario** en Seguridad de las TIC (MISTIC) – UAB

Certificaciones:

- AENOR – Implantador ISO27001
- AENOR – Auditor Líder ISO27001
- IQNet – Auditor Líder ISO27001
- HPE – ATP Hybrid Solutions
- Vmware VMTSP i VSP
- Veeam Backup VMTSP

Consultor y Auditor Interno ENS / ISO27001
Arquitecto de Soluciones TI

INFORDISA

SEGURdades

Colaboro con:

Law&Tech
CYBERCOMPLIANCE

Experiencia en el ENS

Categoría Alta

Consorci d'Aigües de Tarragona

Consell Comarcal del Tarragonès

Categoría Media

Ayuntamiento de Coslada

Ajuntament de Gavà

Madrid Destino

LA NUCIA CIUDAD DEL DEPORTE

AJUNTAMENT DE RIPOLL

AJUNTAMENT DE Vallirana

Ajuntament d'Agramunt

CONSELL COMARCAL DEL VALLÈS OCCIDENTAL

Consell Comarcal de l'Alt Camp

AJUNTAMENT DE SANTA COLOMA DE CERVELLÓ

mmb MUSEU MARITIM DE BARCELONA

INFORDISA

SEGURdades

MASTERTEC

SGRsoft

+ 150 Ayuntamientos

Agenda

Tema 1: **Proceso de Auditoria ENS**

Tema 2: **Fases de una Auditoria del ENS**

Tema 2: **Controles Anexo II - ENS**

Está Regulado

a través de 2 Instrucciones Técnicas de Seguridad en el BOE:

- BOE-A-2018-4573 – Auditoria
- BOE-A-2016-10109 - Conformidad

Guía de Seguridad CCN-STIC
CCN-CERT IC-01/19

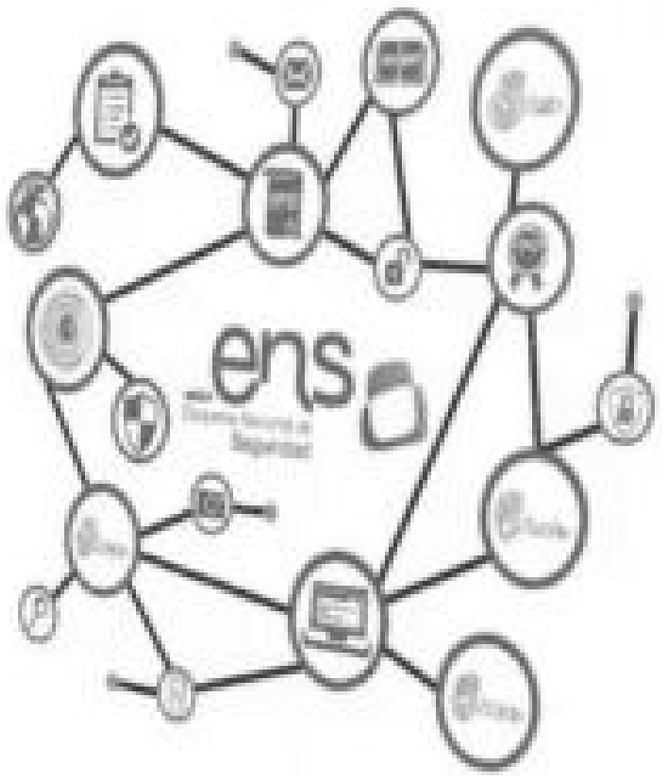
ENS. Criterios Generales de Auditoría y Certificación

Guía del CCN

Guía de Seguridad CCN-STIC

CCN-CERT IC-01/19

- Criterios Generales de Auditoría y Certificación
  - Actualización de Octubre 2023



¿Cuánto dura una auditoria?

Depende de varios factores:

- Complejidad del SI en cuestión
- Tipo de servicios sustentados
- ¿Certificaciones previas? (ENS, 27001...)
- Oficinas y CPDs
- Diversidad tecnológica

Factores de INCREMENTO	Factores de DECREMENTO
• Significativo número de personas con privilegios de administración; • Infraestructura compleja, involucrando varias dependencias o ubicaciones; • Personal que habla más de un idioma (que requiere intérprete o impide que auditores individuales trabajen de forma independiente) o documentación provista en más de un idioma; • Actividades que requieran visitar ubicaciones alternativas o complementarias para confirmar las actividades de las ubicaciones habituales cuyo sistema de gestión está sujeto a certificación.	• Sistemas de Información que soportan Servicios con escaso riesgo; • Sistemas de Información que soportan Servicios de escasa complejidad tecnológica; • Equipos de usuarios sometidos a un mismo control organizacional, desarrollando las mismas tareas; • Conocimiento previo de la organización y del sistema auditado. (Por ejemplo, si el sistema ya ha sido certificado previamente con el ENS); • Experiencia del cliente en las certificaciones de conformidad. (Por ejemplo, sistema ya certificado o reconocido por otro esquema de certificación en materia de seguridad de la información, tal como ISO 27001, por ejemplo); • Elevada madurez del sistema de gestión de seguridad de la información.

20% de variación como máximo

Tiempos de auditoría razonables

Fase de estudio documental previo	Mínimo, entre 0,5 y 1 jornada.
Fase de auditoría modo remoto/in situ	• Categoría BÁSICA: mínimo, 1,5 jornada. • Categoría MEDIA: mínimo, 2,5 jornadas. • Categoría ALTA: mínimo, 3,5 jornadas.
Fase de redacción de informes	Cualquier Categoría: mínimo, **1** jornada que comprenderá la redacción del Informe de Auditoría completo y adecuadamente evidenciado (señalando cada medida auditada); en su caso, evaluación del Plan de Acciones Correctivas (PAC), revisión y decisión del Comité de Certificación.

¿Quién puede certificarme?

ENAC
Entidad Nacional de Acreditación

Distribuida en

Fase 1: Estudio Documental

Fase 2: Auditoria de Cumplimiento

Fase 3: Plan de Acciones Correctivas

Fase 4: Obtención de la Certificación

Di lo que haces

Documentos

Políticas

Normativas

Instrucciones

Manuales

Haz lo que dices

Configuraciones

Mecanismos técnicos

Registros

- Tickets
- Correos electrónicos
- Excels, Words, docs firmados...

Di lo que haces

Documentos

Políticas

Normativas

Instrucciones

Manuales

Fase1: Estudio Documental

- Entender el **Contexto** de la organización
  - Alcance del SGSI, Organigrama, Arquitectura, proveedores...
- Proceso de determinación de la **Categoría del Sistema**
- Proceso de **Gestión de Riesgos**
- **Declaración de Aplicabilidad**
  - Exclusiones, medidas compensatorias, madurez de los controles...
- Informes de **Auditorias previas**
  - Planes de acciones Correctivas
- Revisar actas de Comité, documentos, procedimientos firmados y aprobados formalmente

Listado de documentos de la Fase 1:

1. Alcance (texto que aparecerá en el certificado)
2. Descripción detallada del Sistema de Información que sustenta el Alcance
3. Categoría del sistema según el Anexo I del ENS y procedimiento utilizado.
4. Organigrama de los servicios, departamentos o áreas, con funciones y responsabilidades.
5. Identificación de los roles / responsables del ENS y sus funciones.
6. La Política de Seguridad.
7. La Política de Firma Electrónica.
8. La normativa de seguridad.

Listado de documentos de la Fase 1:

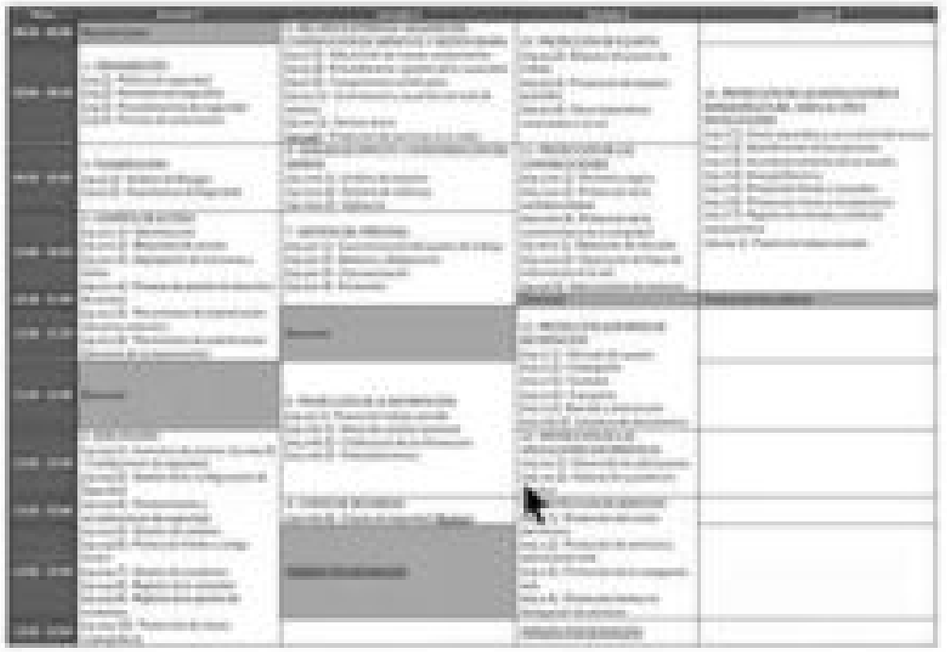
9. Relación documental del Sistema de Gestión que lo sustancia.
10. La Declaración de Aplicabilidad y grado de madurez.
11. Proceso de Gestión del riesgo, metodología usada, Plan de Tratamiento del Riesgo, informes...
12. Informes de auditorías previas (RGPD, ISO27001, Auditorias Internas...)
13. Mapas de red, arquitectura de seguridad y/o descripción básica de alto nivel del SI.
14. Métricas e Indicadores del SGSI establecidos o informe INES (si aplica).
15. Lista de proveedores dentro del Alcance de la auditoría y certificaciones del ENS.
16. Otros Procedimientos para el cumplimiento del ENS

Recomendación:
Ponédselo fácil al Auditor

- Auditar requiere de mucha capacidad de abstracción.
- No conoce absolutamente nada de vuestra organización.
- Hacedle un resumen de presentación claro y conciso.
  - Diagramas, esquemas, tablas, etc....
- Debe de ser capaz de entender bien la organización para elaborar un Plan de Auditoria adecuado.

El Auditor Líder elabora un Plan de Auditoria: Cronograma de la Auditoria

- Horarios y distribución de Jornadas
- Controles del Anexo II
- Auditor asignado para cada control
- Personal Auditado para cada control
- Lugar de Auditoria



Fase 2: Auditoria de Cumplimiento

Objetivo: Verificar y obtener evidencias

Verificar que se cumple lo que indica en los documentos entregados

El auditado debe aportar evidencias del cumplimiento de cada control

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
org	**Marco organizativo**				
org.1	Política de seguridad	Categoría	aplica	aplica	aplica
org.2	Normativa de seguridad	Categoría	aplica	aplica	aplica
org.3	Procedimientos de seguridad	Categoría	aplica	aplica	aplica
org.4	Proceso de autorización	Categoría	aplica	aplica	aplica
op	**Marco operacional**				
op.pl	Planificación				
op.pl.1	Análisis de riesgos	Categoría	aplica	+ R1	+ R2
op.pl.2	Arquitectura de Seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.pl.3	Adquisición de nuevos componentes	Categoría	aplica	aplica	aplica
op.pl.4	Dimensionamiento/gestión de la capacidad	D	aplica	+ R1	+ R1
op.pl.5	Componentes certificados	Categoría	n.a	aplica	aplica
op.acc	Control de acceso				
op.acc.1	Identificación	TA	aplica	+ R1	+ R1
op.acc.2	Requisitos de acceso	CITA	aplica	aplica	+ R1
op.acc.3	Segregación de funciones y tareas	CITA	n.a	aplica	+ R1
op.acc.4	Proceso de gestión de derechos de acceso	CITA	aplica	aplica	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	CITA	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	CITA	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9

4.1.2 Arquitectura de seguridad [op.pl.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R2+R3

Requisitos.

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

– [op.pl.2.1] Documentación de las instalaciones, incluyendo áreas y puntos de acceso.

– [op.pl.2.2] Documentación del sistema, incluyendo equipos, redes internas y conexiones al exterior, y puntos de acceso al sistema (puestos de trabajo y consolas de administración).

– [op.pl.2.3] Esquema de líneas de defensa, incluyendo puntos de interconexión a otros sistemas o a otras redes (en especial, si se trata de Internet o redes públicas en general); cortafuegos, DMZ, etc.; y la utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

– [op.pl.2.4] Sistema de identificación y autenticación de usuarios, incluyendo el uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga, y el uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

Refuerzo R1-Sistema de gestión.

[op.pl.2.r1.1] Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.

Refuerzo R2-Sistema de gestión de la seguridad con mejora continua.

[op.pl.2.r2.1] Sistema de gestión de la seguridad de la información, con actualización y aprobación periódica.

Refuerzo R3-Validación de datos.

[op.pl.2.r3.1] Controles técnicos internos, incluyendo la validación de datos de entrada, salida y datos intermedios.

Tema 2: **Fases de una Auditoria del ENS**

Arquitectura de Seguridad [op.pl.2].

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

– [op.pl.2.1] Documentación de las instalaciones, incluyendo áreas y puntos de acceso.

– [op.pl.2.2] Documentación del sistema, incluyendo equipos, redes internas y conexiones al exterior, y puntos de acceso al sistema (puestos de trabajo y consolas de administración).

– [op.pl.2.3] Esquema de líneas de defensa, incluyendo puntos de interconexión a otros sistemas o a otras redes (en especial, si se trata de Internet o redes públicas en general), cortafuegos, DMZ, etc., y la utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

– [op.pl.2.4] Sistema de identificación y autenticación de usuarios, incluyendo el uso de claves concertadas, contraseñas, puntos de identificación, biometría, u otros de naturaleza análoga, y el uso de firmas o certificados para autenticar al usuario y determinar sus derechos de acceso.

Refuerzos

R1-Sistema de gestión

[op.pl.2.r1.1] Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.

R2-Sistema de gestión de la seguridad con mejora continua

[op.pl.2.r2.1] Sistema de gestión de la seguridad de la información, con actualización y aprobación periódica.

R3-Validación de datos

[op.pl.2.r3.1] Controles técnicos internos, incluyendo la validación de datos de entrada, salida y datos intermedios.

Aplicabilidad

– Categoría BÁSICA: op.pl.2

– Categoría MEDIA: op.pl.2 + R1

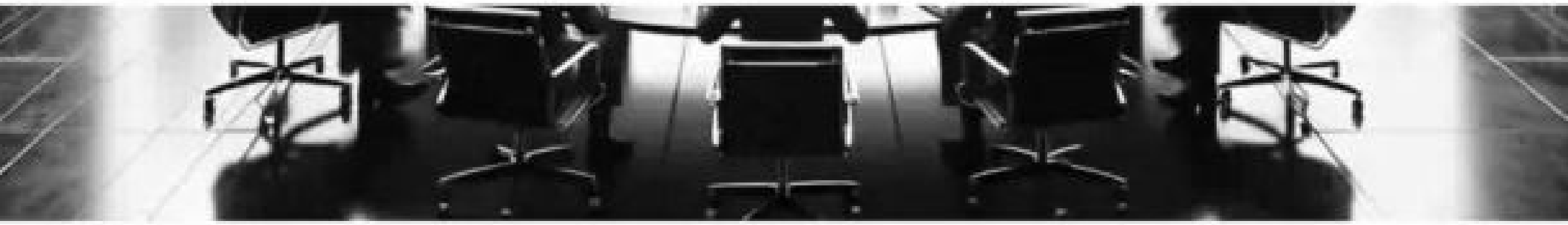
– Categoría ALTA: op.pl.2 + R1 + R2 + R3

Tema 2: **Fases de una Auditoria del ENS**

[illegible]	Dimensiones				CONTROLES ENS		Modelo CMM				[illegible]	[illegible]	Documentos	Requerimientos Técnicos
					Control	Descripción	Objetivo	Estado	Falta	Aplica			ID_Documento	Requerimientos
					MARCO ORGANIZATIVO [illegible]									
					MARCO OPERACIONAL [illegible]									
					PLANIFICACIÓN									
5	DIC AT	aplica	[illegible]	[illegible]	[op.pl.1]	Análisis de Riesgos	3	3	0	[illegible]		X	[illegible] Análisis y Gestión de Riesgos [illegible] Análisis de Riesgos Análisis y Gestión de Riesgos - PILAR	NA
6	DIC AT	aplica	[illegible]	[illegible]	[op.pl.2]	Arquitectura de Seguridad	3	3	0	[illegible]		X	Planos y esquemas de la Entidad -Esquemas de Red Esquemas y documentación de red sobre su configuración [illegible] Inventario de mecanismos de autenticación [illegible] Listado de documentos [illegible]	NA
7	DIC AT	aplica	aplica	aplica	[op.pl.3]	Adquisición de nuevos componentes	3	3	0	[illegible]		X	[illegible] Gestión de proveedores Estudios y análisis previos a la contratación [illegible] de compra	NA
8	D	aplica	[illegible]	[illegible]	[op.pl.4]	Dimensionamiento / Gestión de capacidades	3	3	0	[illegible]		X	[illegible] Configuración Segura de los Sistemas [illegible] Gestión de proveedores Estudio de Dimensionamiento Planes de capacidad	NA
9	[illegible]	n.a	aplica	aplica	[op.pl.5]	Componentes certificados	3	3	0	[illegible]		X	[illegible] Gestión de proveedores [illegible] Listado de productos certificados Catalogo CPSTIC	NA
						Media de los controles [op.pl]		3						
					CONTROL DE ACCESO									
10	AT	aplica	[illegible]	[illegible]	[op.acc.1]	Identificación	3	3	0	[illegible]	X		[illegible] General de uso de recursos y sistemas de la información [illegible]	Active Directory
11	ICA T	aplica	aplica	[illegible]	[op.acc.2]	Requisitos de acceso	3	3	0	[illegible]	X		[illegible] Normativa general de uso de recursos i sistemes d'informació [illegible] Gestión de Usuarios [illegible] Accesos según perfil	[illegible] en Windows y Aplicaciones Permisos por carpetas Grupos de seguridad en el AD
12	ICA T	n.a	aplica	[illegible]	[op.acc.3]	Segregació de funcions y tasques	3	3	0	[illegible]		X	[illegible] Política General de Seguridad de la Información [illegible] General de uso de recursos y sistemas de la información [illegible] Gestión de Usuarios	
13	ICA T	aplica	aplica	aplica	[op.acc.4]	Proceso de gestión de derechos de acceso	3	3	0	[illegible]	X	X	[illegible] General de uso de recursos y sistemas de la información [illegible] Gestión de Usuarios	
14	ICA T	[illegible]	[illegible]	[illegible]	[op.acc.5]	Mecanismo de autenticación (usuarios externos)	3	3	0	[illegible]	X	X	[illegible] General de uso de recursos y sistemas de la información [illegible] Creación y uso de contraseñas [illegible] Gestión de Usuarios [illegible] Inventario de [illegible]	[illegible] VPN, [illegible], GPOs de configuración
15	ICA	[illegible]	[illegible]	[illegible]	[op.acc.6]	Mecanismo de autenticación (usuarios de la organización)	3	3	0	[illegible]	X	X	[illegible] General de uso de recursos y sistemas de la información [illegible] Creación y uso de contraseñas [illegible] Gestión de Usuarios [illegible] Inventario de [illegible] [illegible] Personal autorizado para el acceso a áreas de acceso restringido	GPOs de configuración

Fase 3: Plan de Acciones Correctivas

Objetivo: Resolver las No conformidades



Hallazgos de Auditoria

Favorable

No se hallan No Conformidades Mayores

Hallazgos de Auditoria

Favorable

No se hallan No Conformidades Mayores

Favorable con No Conformidades

Se hallan No Conformidades Mayores o Menores

Elaborar un Plan de Acciones Correctivas

Favorable con No Conformidades

Más de 10 No Conformidades

Requiere de Auditoria Extraordinaria

Plan de Acciones Correctivas

Numero de NC	Proceso	Cláusula	Descripción de la no conformidad	Grado	ANÁLISIS CAUSA RAÍZ (¿Que ha fallado en el sistema para que esta NC ocurra?)	Corrección (Qué se hace para resolver este problema)	Acción Correctiva (Qué se hace para prevenir la repetición)	Fecha de finalización	Rep. de la Organización
NC01									
NC02									
NC03									
NC04									
NC05									

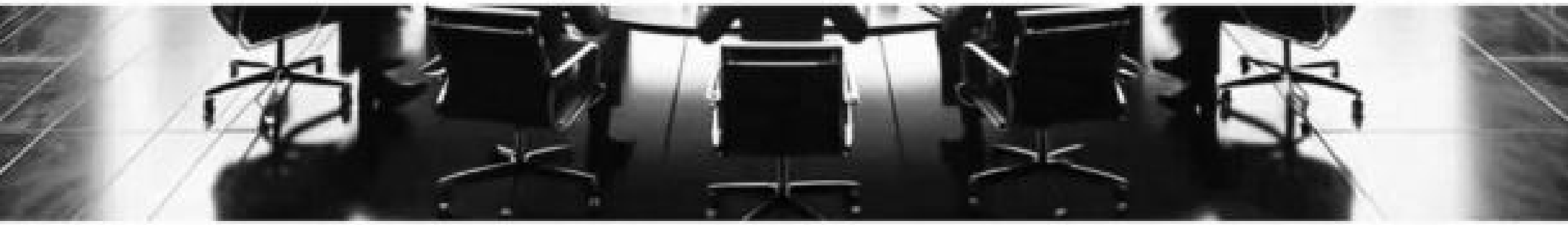
Fase 4 – Obtención de la Certificación

Consejos para la primera **Certificación del ENS**

Fase 4 – Obtención de la Certificación

[op.pl.] Planificación

Antes de la puesta en explotación



Op.pl - Planificación

Op.pl.3 – Adquisición de Nuevos Componentes

Op.pl.4 – Dimensionamiento / Gestión de capacidades

- Definir un Modelo de estudio Previo que incluya:
  - Si está contemplado en el AR
  - Si es acorde a la arquitectura de seguridad
  - Necesidades Técnicas, Formativas, costes económicos
  - Analice las capacidades necesarias
    - (CPU, Disco, RAM, personal, Instalaciones…)
  - Esté elaborado y aprobado por el personal competente

ANTES DE LA ADQUISICIÓN DEL COMPONENTE			
SOLICITA	[Indicar la persona que solicita el análisis]	FECHA	
REALIZA	[Indicar la persona que realiza el análisis]	FECHA	
APRUEBA	[Indicar la persona que aprueba el análisis]	FECHA	
DESCRIPCIÓN DE COMPONENTE A ADQUIRIR			
DESCRIPCIÓN DE LAS ACTIVIDADES PARA LAS CUALES SE PRECISA[2]			

ADQUISICIÓN DE NUEVOS COMPONENTES [op.pl.3]		
	EVALUAR	OBSERVACIONES
RECOGIDO EN PLAN DE TRATAMIENTO DE RIESGOS [op.pl.1]	[SI/NO]	
ES ACORDE LA ARQUITECTURA DE SEGURIDAD [op.pl.2]	[SI/NO]	
ES COMPONENTE CERTIFICADO [op.pl.5]	[SI/NO]	
NECESIDADES		
TÉCNICAS[3]		
FORMATIVAS		
FINANCIACIÓN		

ESTUDIO DE DIMENSIONAMIENTO/GESTIÓN DE CAPACIDAD [op.pl.4]				
	NECESIDADES	JUSTIFICAR (si no hay recursos suficientes)	REALIZA ESTUDIO	FECHA
PROCESAMIENTO [4]				
ALMACENAMIENTO DE INFORMACIÓN [5]				
COMUNICACIÓN[6]				
PERSONAL (CANTIDAD Y CUALIFICACIÓN Y PROFESIONAL) [7]				

¿Tengo que hacer este formulario para absolutamente todas las compras TIC que haga?

¡Sentido común!

Repetiréis muchas compras
(Ordenadores, switches, AP, Servidores…)

Op.pl.5 – Productos Certificados

Medida compensatoria

-Obtener **compromiso del CSI** de adquirir productos certificados en la siguiente renovación.

-**Aumentar la monitorización** sobre estos activos no certificados

-Atención **prioritaria a los CVE** que se detecten

-Realizar un **mantenimiento diligente** de los componentes de estos activos

[op.acc] Control de Acceso

Gestión de los usuarios

Op.acc.1 - Identificación

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

– [op.acc.1.1] Se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación, entre ellos, los sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

– [op.acc.1.2] Cuando el usuario tenga diferentes roles frente al sistema (como ciudadano o usuario final, como trabajador del organismo o como administrador de los sistemas, por ejemplo) recibirá identificadores singulares para cada perfil, de forma que se recaben siempre los correspondientes registros de actividad, delimitándose los privilegios correspondientes a cada perfil.

– [op.acc.1.3] Cada entidad (entidad, usuario o proceso) que accede al sistema, contará con un identificador singular que permita conocer el destinatario de los mismos y los derechos de acceso que recibe, así como las acciones realizadas por cada entidad.

– [op.acc.1.4] Las cuentas de usuario se gestionarán de la siguiente forma:

a) Cada cuenta (de entidad, usuario o proceso) estará asociada a un identificador único.

b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó da orden en sentido contrario.

c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará «periodo de retención».

Op.acc.1 - Identificación

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

– [op.acc.1.1] Se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación, entre ellos, los sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

– [op.acc.1.2] Cuando el usuario tenga diferentes roles frente al sistema (como ciudadano o usuario final, como trabajador del organismo o como administrador de los sistemas, por ejemplo) recibirá identificadores singulares para cada perfil, de forma que se recaben siempre los correspondientes registros de actividad, delimitándose los privilegios correspondientes a cada perfil.

– [op.acc.1.3] Cada entidad (entidad, usuario o proceso) que accede al sistema, contará con un identificador singular que permita conocer el destinatario de los mismos y los derechos de acceso que recibe, así como las acciones realizadas por cada entidad.

– [op.acc.1.4] Las cuentas de usuario se gestionarán de la siguiente forma:

a) Cada cuenta (de entidad, usuario o proceso) estará asociada a un identificador único.

b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó da orden en sentido contrario.

c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará «periodo de retención».

Op.acc.1 - Identificación

Refuerzo R1-Identificación avanzada.

– [op.acc.1.r1.1] La identificación del usuario permitirá al Responsable del Sistema, al Responsable de la Seguridad o a sus respectivos administradores delegados, singularizar a la persona asociada al mismo, así como sus responsabilidades en el sistema.

– [op.acc.1.r1.2] Los datos de identificación serán utilizados por el sistema para determinar los privilegios del usuario conforme a los requisitos de control de acceso establecidos en la documentación de seguridad.

– [op.acc.1.r1.3] Se asegurará la existencia de una lista actualizada de usuarios autorizados y mantenida por el administrador del sistema/de la seguridad del sistema.

Op.acc.1 - Identificación

Consejos:

2 perfiles para los sysadmin:
- Usuario de login al PC (*jvidal*)
- Usuario privilegiado (*ajvidal*)

Prohibido usar *administrador@dominio* para todo y para todos!
- Los servicios, identificados en el AD (Veeam, Sage, Sophos...)
- Los proveedores, también!

No dejar los usuarios deshabilitados en el AD eternamente.
Establecer un periodo de retención (1 mes, 3 meses, 1 año...)

Aplica tanto en máquinas Windows, Linux, Unix, Firewalls...

Op.acc.2 Requisitos de acceso

Requisitos.

– [op.acc.2.1] Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.

– [op.acc.2.2] Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.

– [op.acc.2.3] Particularmente, se controlará el acceso a los componentes del sistema operativo y a sus ficheros o registros de configuración.

Refuerzo R1-Privilegios de acceso.

– [op.acc.2.r1.1] Todos los usuarios autorizados deben tener un conjunto de atributos de seguridad (privilegios) que puedan ser mantenidos individualmente.

– [op.acc.2.r1.2] Los privilegios de acceso se implementarán para restringir el tipo de acceso que un usuario puede tener (lectura, escritura, modificación, borrado, etc.).

Op.acc.4 Proceso de gestión de derechos de acceso

Los derechos de acceso de cada entidad, usuario o proceso se limitarán atendiendo a los siguientes principios:

- [op.acc.4.1] Todo acceso estará prohibido, salvo autorización expresa.

- [op.acc.4.2] Mínimo privilegio: los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones.

- [op.acc.4.3] Necesidad de conocer y responsabilidad de compartir: los privilegios se asignarán de forma que las entidades, usuarios o procesos sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones. La información es patrimonio del organismo y toda aquella que resulte necesaria para el usuario estará a su disposición.

- [op.acc.4.4] Capacidad de autorizar: Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable. Los permisos de acceso se revisarán de forma periódica.

- [op.acc.4.5] Se establecerá una política específica de acceso remoto, requiriéndose autorización expresa.

Op.acc.4 Proceso de gestión de derechos de acceso

Los derechos de acceso de cada entidad, usuario o proceso se limitarán atendiendo a los siguientes principios:

- [op.acc.4.1] Todo acceso estará prohibido, salvo autorización expresa.

- [op.acc.4.2] Mínimo privilegio: los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones.

- [op.acc.4.3] Necesidad de conocer y responsabilidad de compartir: los privilegios se asignarán de forma que las entidades, usuarios o procesos sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones. La información es patrimonio del organismo y toda aquella que resulte necesaria para el usuario estará a su disposición.

- [op.acc.4.4] Capacidad de autorizar: Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable. Los permisos de acceso se revisarán de forma periódica.

- [op.acc.4.5] Se establecerá una política específica de acceso remoto, requiriéndose autorización expresa.

Op.acc.2 y Op.acc.4

Consejos:

Interconectar con los controles **[org.4] Proceso de Autorización** y **[op.exp.1] Inventario de activos**:
- Utilizar el mismo proceso de autorización (ticket, correo, etc).
- El responsable indicado en el inventario es quien debe autorizar el acceso

Op.acc.4 Proceso de gestión de derechos de acceso

Los derechos de acceso de cada entidad, usuario o proceso se limitarán atendiendo a los siguientes principios:

- [op.acc.4.1] Todo acceso estará prohibido, salvo autorización expresa.

- [op.acc.4.2] Mínimo privilegio: los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones.

- [op.acc.4.3] Necesidad de conocer y responsabilidad de compartir: **los privilegios se asignarán de forma que las entidades, usuarios o procesos sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones. La información es patrimonio del organismo y toda aquella que resulte necesaria para el usuario estará a su disposición.**

- [op.acc.4.4] Capacidad de autorizar: **Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable. Los permisos de acceso se revisarán de forma periódica.**

- [op.acc.4.5] Se establecerá una política específica de acceso remoto, **requiriéndose autorización expresa.**

Op.acc.2 y Op.acc.4

Consejos:

Interconectar con los controles **[org.4] Proceso de Autorización** y **[op.exp.1] Inventario de activos**:
- Utilizar el mismo proceso de autorización (ticket, correo, etc).
- El responsable indicado en el inventario es quien debe autorizar el acceso

Crear una matriz de personas con capacidad de autorizar (Carpetas departamentales, aplicaciones, etc)
Crear una matriz de permisos mínimos según perfil (Comercial, Técnico, Administración, Dirección...).

Op.acc.2 y Op.acc.4

Consejos:

Interconectar con los controles **[org.4] Proceso de Autorización** y **[op.exp.1] Inventario de activos**:
- Utilizar el mismo proceso de autorización (ticket, correo, etc).
- El responsable indicado en el inventario es quien debe autorizar el acceso

Crear una matriz de personas con capacidad de autorizar (Carpetas departamentales, aplicaciones, etc)
Crear una matriz de permisos mínimos según perfil (Comercial, Técnico, Administración, Dirección...).

Op.acc.2 y Op.acc.4

Consejos:

Interconectar con los controles **[org.4] Proceso de Autorización** y **[op.exp.1] Inventario de activos**:
- Utilizar el mismo proceso de autorización (ticket, correo, etc).
- El responsable indicado en el inventario es quien debe autorizar el acceso

Crear una matriz de personas con capacidad de autorizar (Carpetas departamentales, aplicaciones, etc)
Crear una matriz de permisos mínimos según perfil (Comercial, Técnico, Administración, Dirección...).

Utilizar los grupos (*Active Directory*) para gestionar los permisos.
Pedir periódicamente al responsable del activo que valide las personas de dicho grupo (miembros).

```
Get-ADGroupMember -Identity "Comerciales" -Recursive | Select-Object Name | Out-File -FilePath comerciales.txt
```

Op.acc.5-6 – Mecanismo de Autenticación

Consejos:

Activar Doble factor para:
- VPN
- Correo electrónico

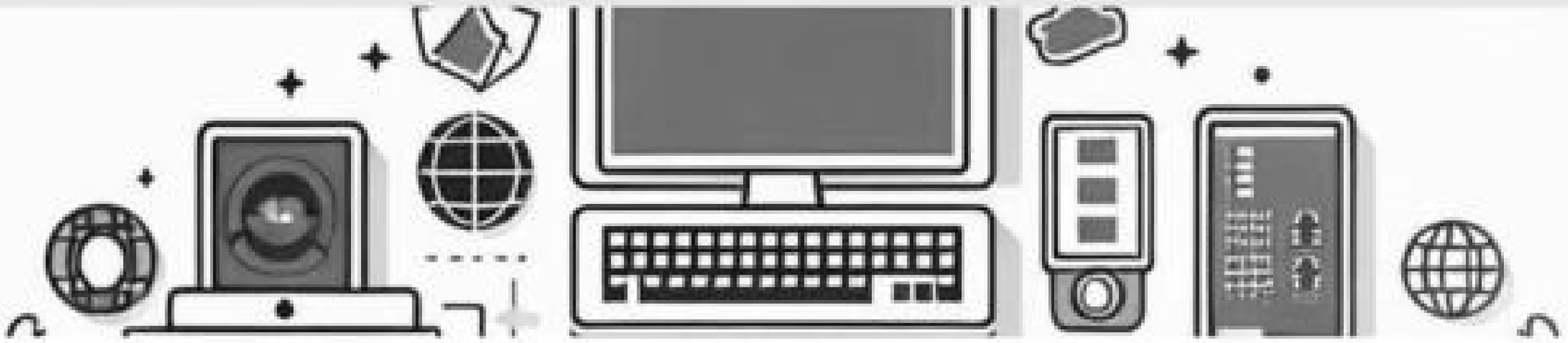
Evitar al máximo posible usuarios tienen la casilla "la contraseña nunca cambia":
- Excepciones (servicios, Administradores de dominio).
  - Realizar el cambio manual y planificado.

Op.acc – Control de Accesos

Consejo General:

Integrar todas las aplicaciones con el AD:
- VPN
- Correo electrónico
- ERP
- CRM

Evitar integrar los Administradores (vCenter, Firewall, aplicaciones...)



[op.exp] Explotación

Gestión de los activos y configuraciones

Op.exp.2 – Configuración segura

Se configurarán los equipos previamente a su entrada en operación, de forma que:

- [op.exp.2.1] Se retiren cuentas y contraseñas estándar.
- [op.exp.2.2] Se aplicará la regla de «mínima funcionalidad», es decir:

a) El sistema debe proporcionar la funcionalidad mínima imprescindible para que la organización alcance sus objetivos.

b) No proporcionará funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su perímetro de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue.

- [op.exp.2.3] Se aplicará la regla de «seguridad por defecto», es decir:

a) Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.

b) Para reducir la seguridad, el usuario tendrá que realizar acciones conscientes.

c) El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

- [op.exp.2.4] Las máquinas virtuales estarán configuradas y gestionadas de un modo seguro. La gestión del parcheado, cuentas de usuarios, software antivirus, etc. se realizará como si se tratara de máquinas físicas, incluyendo la máquina anfitriona.

Op.exp.2 – Configuración segura

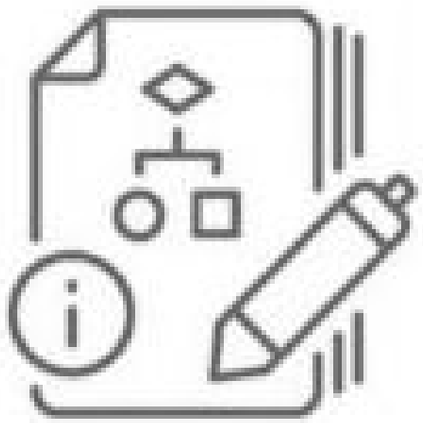
GPOs de Windows

Op.exp.2 – Configuración segura

Consejo:

Haced vuestro propio manual + Checklist basado en:

Guías CCN-STIC



CIS Center for Internet Security®

Creating Confidence in the Connected World.

- 500 Entornos Windows
- 600 Otros entornos

Op.exp.2 – Configuración segura

Manuales CISecurity gratuitos:

Op.exp.2 – Configuración segura

Ejemplo de checklist:

	HARDENING - CLARA
☐	S'ha deixat un Administrador Local als equips PCs diferent a l'usuari "ADMINISTRADOR".
☐	L'usuari no és administrador local de l'Equip.
☐	S'han re-anomenat els usuaris "administrador" i "invitado" per defecte dels Equips. i s'han deshabilitat.
☐	La política de contrasenyes s'ha configurat adequadament segons les indicacions.
☐	UAC està activat.
☐	Firewall Està activat.
☐	Windows Defender (o antivirus propi) està activat.
☐	Claus de Registres SMB aplicades.
☐	Deshabilitar Permitir Todos los Scripts de powershell.

Op.exp.3 – Gestión de la configuración

Se gestionará de forma continua la configuración de los componentes del sistema, de forma que:

- [op.exp.3.1] Se mantenga en todo momento la regla de "funcionalidad mínima" ([op.exp.2]).
- [op.exp.3.2] Se mantenga en todo momento la regla de "mínimo privilegio" ([op.exp.2]).
- [op.exp.3.3] El sistema se adapte a las nuevas necesidades, previamente autorizadas. (Ver [op.acc.4]).
- [op.exp.3.4] El sistema reaccione a vulnerabilidades notificadas. (Ver [op.exp.4]).
- [op.exp.3.5] El sistema reaccione a incidentes. (Ver [op.exp.7]).
- [op.exp.3.6] La configuración de seguridad solamente podrá editarse por personal debidamente autorizado.

Refuerzo R1-Mantenimiento regular de la configuración.

- [op.exp.3.r1.1] Existirán configuraciones hardware/software, autorizadas y mantenidas regularmente, para los servidores, elementos de red y estaciones de trabajo.
- [op.exp.3.r1.2] Se verificará periódicamente la configuración hardware/software del sistema para asegurar que no se han introducido ni instalado elementos no autorizados.
- [op.exp.3.r1.3] Se mantendrá una lista de servicios autorizados para servidores y estaciones de trabajo.

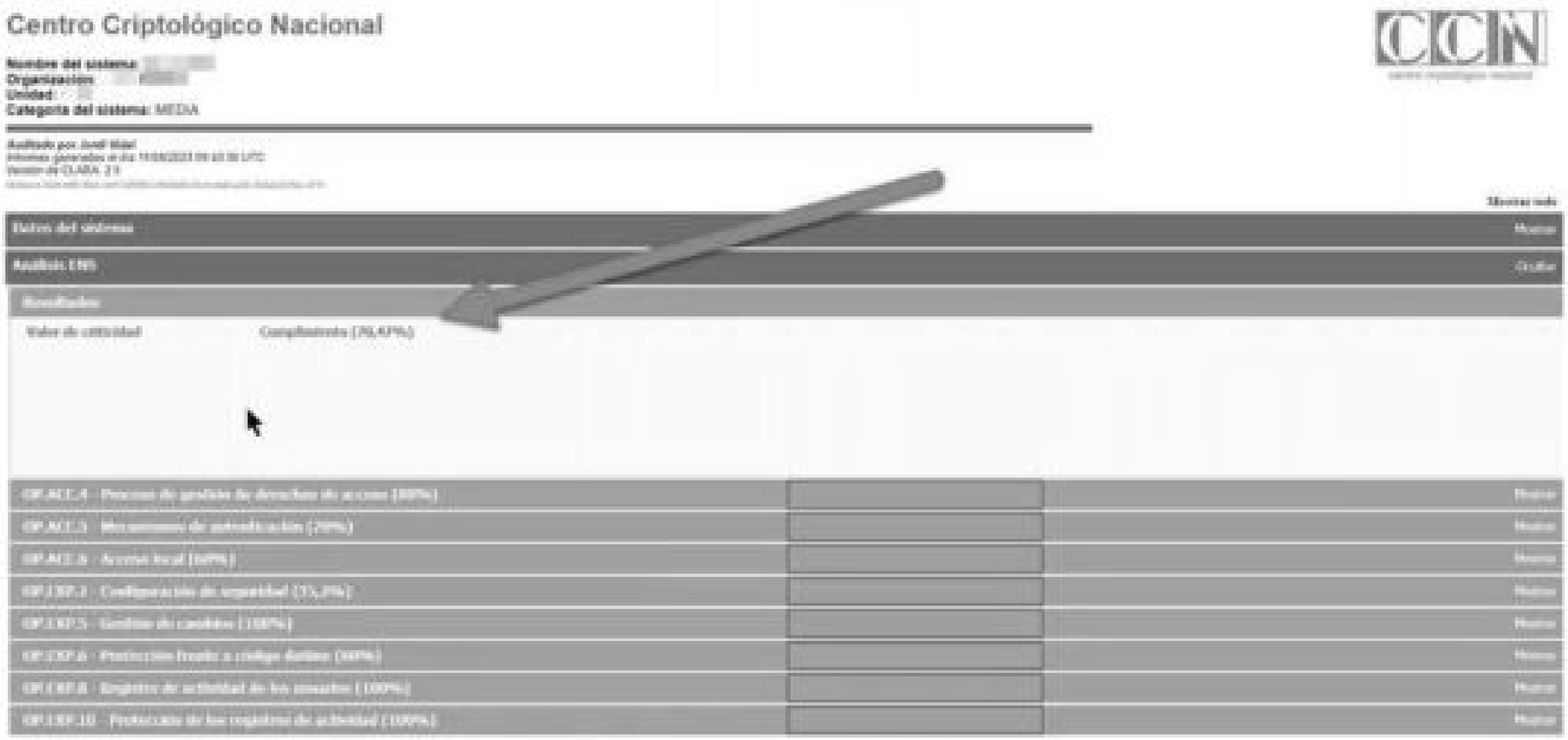
Op.exp.3 – Gestión de la configuración

Windows (Pcs)	Microsoft	Sistema Operatiu	Windows 10 Pro
Windows Server	Microsoft	Sistema Operatiu Servidors	Windows Server 2019
Suite Office	Microsoft	Ofimàtica	Windows Server 2019
Acrobat Reader	Adobe	PDFs	Última disponible
ESET Endpoint Antivirus	NOD32	Antivirus	Última disponible
Google Earth Pro	Google	planificació rutes tècniics	7.3.6.9345
AutoFirma	Gobierno de España	Firma documents	1.7.2
Bit4id - Universal MW 1.4.10.66	Bit4id	firma documents	1.4.10.667
SafeSign 64-bits	A.E.T. Europe B.V.	firma documents	3.0.76
Chrome	Google	Navegador	Última disponible
Firefox	Mozilla	Navegador	Última disponible
Edge	Microsoft	Navegador	Última disponible
7-zip	Igor Pavlov	comprimir/descomprimir	Última disponible
Winrar	On-Line Services 2000, S.L.	comprimir/descomprimir	Última disponible
VLC Media Player	VideoLAN	Reproductor Multimedia	Última disponible
CutePDF Writer	Acro Software Inc.	PDFs	Última disponible
Logitech SyncAgent	Logitech Europe S.A.	Drivers Logitech	Última disponible
Ivanti Secure Access Client 22.2	Ivanti, Inc.	VPN	22.2.1295
Pulse Application Launcher	Ivanti, Inc.	VPN	22.3.18209
Sophos Connect	Sophos	Client VPN	Última disponible

Op.exp.3 – Gestión de la configuración

CLARA ENS [Descarga] Contraseña: CLARA | Firma SHA [Descarga]
CLARA ENS Linux [Descarga] Contraseña: CLARA | Firma SHA [Descarga]

Op.exp.3 – Gestión de la configuración



Op.exp.4 – Mantenimiento y actualizaciones de seguridad

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

– [op.exp.4.1] Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos.

– [op.exp.4.2] Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la implantación o no de la actualización.

– [op.exp.4.3] El mantenimiento solo podrá realizarse por personal debidamente autorizado.

Refuerzo R1-Pruebas en preproducción.

[op.exp.4.r1.1] Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un entorno de prueba controlado y consistente en configuración al entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

Op.exp.4 – Mantenimiento y actualizaciones de seguridad

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

– [op.exp.4.1] Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos.

– [op.exp.4.2] Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la implantación o no de la actualización.

– [op.exp.4.3] El mantenimiento solo podrá realizarse por personal debidamente autorizado.

Refuerzo R1-Pruebas en preproducción.

[op.exp.4.r1.1] Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un entorno de prueba controlado y consistente en configuración al entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

Op.exp.4 – Mantenimiento y actualizaciones de seguridad

Consejos:

Op.exp.4 – Mantenimiento y actualizaciones de seguridad

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

– [op.exp.4.1] Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos.

– [op.exp.4.2] Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la implantación o no de la actualización.

– [op.exp.4.3] El mantenimiento solo podrá realizarse por personal debidamente autorizado.

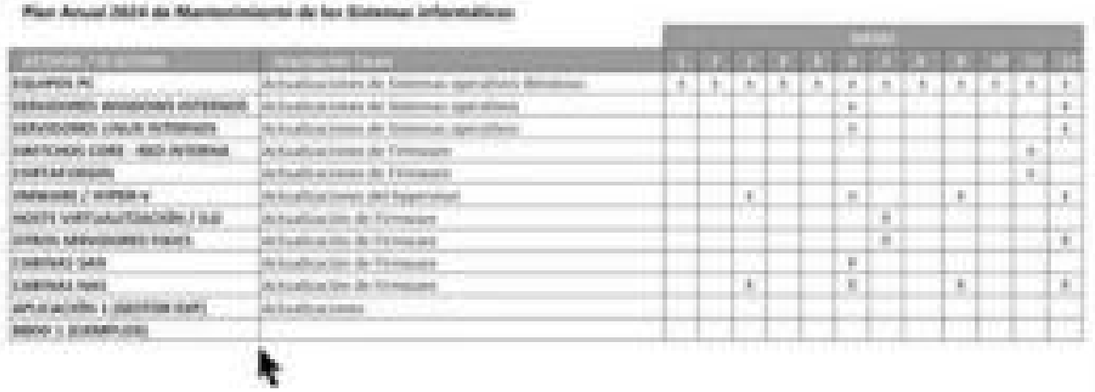
Refuerzo R1-Pruebas en preproducción.

[op.exp.4.r1.1] Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un entorno de prueba controlado y consistente en configuración al entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

Op.exp.4 – Mantenimiento y actualizaciones de seguridad

Consejos:

- **Plan de Mantenimiento anual**



- **Subscripciones a boletines de seguridad**
  - (RSS CCN, Fabricantes, soc.Infordisa.com)

- **R1 - Entorno Preproducción**
  - **Entorno virtualizado?**
    - Clonar VMs y actualizar
  - **Entorno redundante?**
    - Actualizar pasivo primero
  - **No tenemos nada de lo anterior?**
    - Define siempre un Rollback

Op.exp.5 – Gestión del cambio

Consejos:

Cambio crítico

- RFC ITIL
- Riesgos identificados
- Pruebas de aceptación
- Pentest / Análisis Vulnerabilidad
- Backup / Snapshot previo
- Ventana ejecución
- Ticket resultados

Cambio preautorizado

- Backup / Snapshot previo
- Ventana ejecución
- Ticket resultados

Op.cont.1 – Análisis de Impacto

4.6.1 Análisis de impacto [op.cont.1].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [op.cont.1.1] Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado), así como los elementos que son críticos para la prestación de cada servicio.

Aplicación de la medida (por disponibilidad).

Op.cont.1 – Análisis de Impacto

Consejos:
Coherencia con la dimensión **[D] DISPONIBILIDAD** en la Valoración y categoría establecida!

Op.cont.1 – Análisis de Impacto

Consejos:

Coherencia con la dimensión **[D] DISPONIBILIDAD** en la Valoración y categoría establecida!

CRITERIOS PARA LA DISPONIBILIDAD DE SERVICIOS				
	No Aplicable (N/A)	**BAJO**	**MEDIO**	**ALTO**
RTO – Tiempo Objetivo de Recuperación	DIS.RTO.N La restauración de los niveles mínimos de servicio puede realizarse en un plazo superior a 5 días (RTO)	DIS.RTO.B La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 5 días (RTO)	DIS.RTO.M La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 1 día (RTO)	DIS.RTO.A La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 4 horas (RTO)

ANÁLISIS DE IMPACTO EN EL NEGOCIO - (BIA)	REG-ENS-002
Documento de uso interno	Versión 1.0

ID Servicio	Nombre Actividad/Proceso	Area/Departamento	Nombre Responsable	Categoria ENS	Impacto al Negocio					REQUISITO NEGOCIO	
					15 min	1 hora	4 horas	1 día	5 días	RTO	RPO
S01	Cloud Privado	Informática	Responsable Sistema	ALTA	2	3	4	4		1H	4H
S02	Administración	Administración	CEO	MEDIA	0	1	3	4		16H	24H
S03	Comercial	Comercial	director comercial	BAJA	0	0	1	2		2H	24H

Muchas gracias por vuestra atención

INFORDISA

Jordi Vidal

Solutions Architect

jvidal@infordisa.com

693 799 798

Carrer del Tren, 4
43800 Valls (Tarragona)

977 600 321

infordisa.com