INSTRUCCIONES:

El siguiente cuestionario pretende ampliar el conocimiento de los sistemas de información de la entidad, enmarcado dentro de las actividades de planificación de la auditoría realizada por la Sindicatura / Cámara de Cuentas.

La información obtenida a través del presente cuestionario servirá de base para futuros trabajos, en los que sólo será necesaria su actualización.

Para cumplimentar el cuestionario no es necesario que se genere documentación adicional a la ya disponible. La idea es la de disponer de la documentación ya existente en la entidad en el momento de inicio del trabajo de campo, con el fin de optimizar el tiempo invertido por ambas partes.

El trabajo de campo se desarrollará principalmente mediante entrevistas, de las que podrán surgir necesidades adicionales de información.

En el caso de que exista documentación descriptiva de los procedimientos, no es necesaria la cumplimentación del cuestionario respecto a esos aspectos, basta con la aportación del documento descriptivo.

Del mismo modo, no es imprescindible que nos facilite aquella información que considere puede ser de carácter confidencial. En esos casos indíquelo en el cuestionario y prepárela para el inicio del trabajo.

El alcance de la revisión posee un carácter general, no siendo necesario obtener una información exhaustiva de cada uno de los puntos incluidos en el cuestionario.

Para cualquier duda, no dude en ponerse en contacto con los miembros del equipo de fiscalización (Correo electrónico: XXX@xx.xx, tf. xxx).

Le rogamos nos facilite el cuestionario cumplimentado lo antes posible.

Una vez cumplimentado se devolverá como un documento ***.docx o *.pdf firmado electrónicamente (preferentemente) o en soporte papel con firma hológrafa del responsable del área de sistemas de información.**

CUMPLIMENTADO POR:

Entidad:

Denominación del Departamento TI:

Nombre:

Cargo:

Fecha:

Firma:

Domicilio del Departamento TI:

INFORMACIÓN GENERAL SOBRE EL ENTORNO TECNOLÓGICO DE LA ENTIDAD

Documentación necesaria:

- Copia del mapa de red
- Diagramas de la arquitectura física/lógica de los sistemas de información de la Entidad

En caso de no disponer de dicha documentación, incluir una breve explicación del entorno de TI de la Entidad (existencia o no de DMZ, de segmentación entre red de usuarios y red de servidores, elementos de seguridad (firewall, IPS, etc.), relación de los principales sistemas ubicados en la red interna, uso de soluciones de virtualización, etc.).

A1 - CBCS 8 CUMPLIMIENTO DE LEGALIDAD

8.1.- Esquema Nacional de Seguridad

- ¿Dispone de una política de seguridad escrita?
- ¿Ha sido aprobada por el órgano superior competente (conforme al Art. 11 del RD 3/2010)?
- ¿Se han asignado los siguientes roles/responsabilidades? En caso afirmativo indicar nombre y puesto de la persona a quien se le ha asignado.
  - Responsable/s de la información
  - Responsable/s del servicio
  - Responsable de la seguridad (STIC)
  - Responsable del sistema (TIC)
- ¿Se ha realizado la auditoría de cumplimiento del ENS para los sistemas de categoría Media y Alta? En caso afirmativo, indicar la empresa encargada de la realización de la auditoría.
- Para los sistemas de categoría Básica, ¿se ha realizado la autoevaluación de cumplimiento exigida en el ENS o bien, de forma opcional, la auditoría de cumplimiento?
- Los resultados de la auditoría y de la autoevaluación ¿han sido revisados por el responsable de seguridad y las conclusiones presentadas al responsable del sistema para que adopte las medidas correctoras adecuadas?
- ¿Facilita los datos necesarios para el Informe del Estado de la Seguridad a través de la herramienta INES, cumpliendo así la Instrucción Técnica de Seguridad aprobada por resolución de 7 de octubre de 2016 ?

8.2.- LOPD/RGPD

- ¿Se ha designado Delegado de Protección de Datos (DPD)? En caso afirmativo indicar nombre y puesto de la persona designada, indicando su posición en el organigrama general de la entidad.
- ¿Se ha comunicado su designación a la Agencia Española de Protección de Datos?
- ¿Se dispone de Registro de actividades de tratamiento, de acuerdo a lo establecido en el artículo 30 del RGPD?
- Se han realizado los analisis de riesgo de los tratamientos de datos personales realizados por la entidad y las evaluaciones de impacto para aquellos de riesgo alto?
- ¿Cómo evalúa y verifica la entidad la eficacia de las medidas técnicas y organizativas (ej. mediante auditorías realizadas por empresas externas, autoevaluaciones de cumplimiento, etc.).

8.3.- Ley de Impulso de la factura electrónica y creación del registro contable de facturas)

- ¿Se dispone del informe de auditoría anual de sistemas exigido por la Ley 25/2013, de 27 de diciembre de Impulso de la factura electrónica y creación del registro contable de facturas?

8.4.- Cumplimiento del Esquema Nacional de Interoperabilidad

- ¿Se encuentran los sistemas adecuados a los criterios y recomentaciones establecidos en el Esquema Nacional de Interoperabilidad (Disposición transitoria RD 4/2010)?
- En su defecto, ¿existe el Plan de Adecuación al Esquema Nacional de Interoperabilidad y se encuentra formalmente aprobado?

Documentación necesaria:

- Copia de la Política de seguridad requerida por el ENS
- Copia de los registros (ej. resoluciones, actas, etc.) correspondientes a la designación de los responsabes de la información, del servicio, de seguridad y del sistema según el ENS
- Copia de la informe de auditoría de cumplimiento del ENS para los sistemas de categoría Media y Alta
- Copia de la autoevaluación de cumplimiento para los sistemas de categoría Básica según ENS
- Copia del documento que recoge los datos de la última declaración en la herramienta INES
- Copia de la designación del Delegado de Protección de Datos
- Copia del registro de actividades de tratamiento de datos de carácter personal
- Copia de los analisis de riesgos y evaluaciones de impacto de los tratamientos de datos personales
- En los casos en los que aplique, copia del informe de auditoría o de la autoevaluación de la eficacia de las medidas de seguridad aplicadas a los datos personales
- Copia del informe de auditoría de sistemas exigido en el Art. 12.3. de la Ley 25/2013, de 27 de diciembre de Impulso de la factura electrónica y creación del registro contable de facturas
- Copia del Plan de Adaptación al Esquema Nacional de Interoperabilidad

A.2: ESTRATEGIA DE SEGURIDAD

A.2.1: Planificación estratégica de los SI

- ¿Existe un Plan Estratégico de los Sistemas de TI?

A.2.1: Planificación Anual de Proyectos de SI

- ¿Existe un Plan Anual de Proyectos de SI?

A.2.1: Dotación Presupuestaria para Proyectos de SI

- ¿Existe dotación presupuestaria para los proyectos incluidos en el Plan Anual de Proyectos deSI?

Documentación necesaria:

- Copia del Plan Estratégico de Sistemas de Información
- Copia del Plan Anual de Proyectos e Inversión en TI
- Evidencia de las partidas presupuestarias dedicadas a las inversiones de TI

A.3: ORGANIZACIÓN Y PERSONAL DE TI

A.3.1: Independencia Funcional

- ¿Es el departamento de sistemas de información independiente de otras áreas funcionales?
- ¿Depende el departamento de sistemas de información directamente de la dirección?

A.3.2: Segregación de Funciones

- ¿Existe segregación de funciones y tareas?
- En caso afirmativo, ¿se separan como mínimo las siguientes funciones?
  - Operaciones
  - Administración (configuración, mantenimiento)
  - Supervisión (auditoría, gobierno)

A.3.3: Formación y Concienciación

- ¿Se realizan acciones para concienciar regularmente al personal acerca de su papel y responsabilidad sobre la seguridad de los sistemas y la información contenida en ellos?
- ¿Forma parte del contenido de las acciones de concienciación la normativa de seguridad relativa al buen uso de los sistemas?
- ¿Se forma regularmente al personal en aquellas materias relativas a la seguridad de la información y de los sistemas que le sean de aplicación para el desempeño de sus funciones?

A.3.4: Indicadores de Cumplimiento de Objetivos

- ¿Se utilizan indicadores por parte de la dirección para valorar el cumplimiento de objetivos estratégicos de TI?

A.3.5: Nombramientos y Constitución de Órganos

- ¿Se han realizado los nombramientos requeridos para asegurar el cumplimiento normativo y organización de la seguridad?
- ¿Se han constituido los órganos de gobierno necesarios para asegurar el cumplimiento normativo y organización de la seguridad?

Documentación necesaria:

- Organigrama general de la entidad (incluyendo el área de tecnología).
- Organigrama del área de tecnología.
- Documento de funciones y responsabilidades de cada una de las subáreas de tecnología.
- Copia del Plan de Formación.
- Copia del Plan de Concienciación.
- Documentación acreditativa del uso de indicadores de cumplimiento en los objetivos estratégicos de TI por parte de la dirección.
- Copia de las Acta de Nombramiento de los roles de seguridad.
- Copia de las Acta de Constitución de los Órganos de Gobierno de Seguridad

A.4: MARCO NORMATIVO Y PROCEDIMENTAL DE SEGURIDAD

A.4.1: Normativa Interna de Seguridad

- ¿Dispone de uno o varios documentos que constituyan la Normativa de Seguridad de la Entidad?
- ¿Dicha normativa, especifica cual es el uso correcto de equipos, servicios, instalaciones y sistemas?
- ¿Especifica dicha normativa la responsabilidad del personal con respecto al cumplimiento o violación de estas normas, incluyendo derechos, deberes y medidas disciplinarias?

A.4.2: Procedimientos de Seguridad

- ¿Dispone de uno o varios documentos que constituyan los procedimientos de seguridad escritos?
- ¿Precisan los procedimientos cómo llevar a cabo las tareas habituales?
- ¿Precisan los procedimientos quíen debe realizar cada tarea?

Documentación necesaria:

- Copia de la Normativa Interna de Seguridad.
- Copia de los Procedimientos de Seguridad aprobados.

B.1: ADQUISICIÓN DE APLICACIONES Y SISTEMAS

B.1.1: Procedimiento de Adquisición de Aplicaciones y Sistemas

- ¿Existe un procedimiento formal para planificar y ejecutar la adquisición de nuevas aplicaciones, sistemas o componentes de sistemas?
- ¿El Procedimiento de Adquisición de Aplicaciones y Sistemas tiene en consideración los objetivos de seguridad definidos por la entidad? ¿De qué forma se articula dicha consideración?

B.1.2: Adquisición de Aplicaciones y Sistemas por Objetivos Estratégicos y de Seguridad

- ¿El Procedimiento de Adquisición de Aplicaciones y Sistemas tiene en consideración los objetivos estratégicos y de negocio de la entidad? ¿De qué forma se articula dicha consideración?

B.1.3: Dimensionamiento en la Adquisición de Aplicaciones y Sistemas

- ¿El Procedimiento de Adquisición de Aplicaciones y Sistemas incluye el dimensionamiento adecuado considerando las necesidades actuales y futuras?
- En caso afirmativa, ¿se considera para el dimensionamiento las necesidades relativas lo siguiente?
  - necesidades de procesamiento
  - necesidades de almacenamiento
  - necesidades de comunicación
  - necesidades de personal
  - de instalaciones y medios auxiliares

B.1.4: Adquisición de Aplicaciones y Sistemas Evaluadas desde el punto de vista de la Seguridad

- De acuerdo al Procedimiento de Adquisición de Aplicaciones y Sistemas ¿se utilizan adquieren, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales?

Documentación necesaria:

- Copia del procedimiento Adquisisión de Aplicaciones y Sistemas
- Copia de estudios previos a la adquisición de aplicaciones o sistemas adquiridos

B.2: DESARROLLO DE APLICACIONES

Identifique las aplicaciones que soportan los principales procesos de negocio.

Clasifique cada una de las aplicaciones identificadas según la siguiente taxonomía:

- Software propio desarrollado por la organización.
- Software comprado con pequeñas o ninguna personalización.
- Software comprado con personalización significativa.
- Software propiedad de una empresa de Outsourcing.

B.2.1: Metodología de Desarrollo

- ¿Se utiliza una metodología de desarrollo reconocida para el desarrollo de aplicaciones y sistemas? ¿Cuál es la metodología utilizada?
- En caso afirmativo, ¿considera dicha metodología la seguridad de forma integral a lo largo del ciclo de desarrollo?
- En caso contrario, ¿realiza durante el ciclo de vida del desarrollo las siguiente actividades?:
    - Análisis de requisitos
    - Análisis de viabilidad
    - Diseño seguro
    - Construcción y pruebas
    - Diseño de la puesta en explotación y aceptación

B.2.2: Entornos de Desarrollo

- ¿Se desarrollan las aplicaciones o sistema sobre un entorno diferente y separado del de producción?

B.2.3: Aceptación y puesta en servicio

- ¿Dispone de un plan de pruebas antes de pasar a producción para comprobar el correcto funcionamiento de la aplicación?
- En caso afirmativo, ¿incluye dicho plan pruebas de seguridad como criterios de aceptación?
- ¿Se requiere de la aprobación del usuario en las pruebas de testeo previamente al paso a producción?
- ¿Se realizan las pruebas en un entorno aislado o en el entorno de producción?

Documentación necesaria:

- Copia del procedimiento o metodología utilizada para el desarrollo de sistemas y aplicaciones.
- Ejemplo de documentación generada en el ciclo de vida de dasarrollo de un sistema.

B.3: GESTIÓN DE CAMBIOS

B.3.1: Procedimientos para la gestión de cambios de configuración del sistema

- ¿Se gestiona de forma continua la configuración de aplicaciones y sistemas?
- En caso afirmativo ¿existe un procedimiento para ello?
- ¿Se utiliza alguna herramienta para automatizar la gestión de cambios en la configuración de los sistemas?
- ¿Contempla el procedimiento o la práctica común de los cambios de configuración los siguientes puntos?:
    - Registro de solicitudes
    - Evaluación
    - Autorización
    - Pruebas
    - Planificación de puesta en operación
    - Registro de cambios
- ¿La evaluación del cambio incluye el análisis del riesgo desde el punto de vista de la seguridad?

B.3.2: Procedimientos para la gestión de cambios de componentes o arquitectura del sistema

- ¿Se gestionan de forma continua los cambios de componentes y/o arquitectura de aplicaciones y sistemas?
- En caso afirmativo ¿existe un procedimiento para ello?
- ¿Contempla el procedimiento o la práctica común de los cambios de de componentes y/o arquitectura los siguientes puntos?:
    - Registro de solicitudes
    - Evaluación
    - Autorización
    - Pruebas
    - Planificación de puesta en operación
    - Registro de cambios
- ¿La evaluación del cambio incluye el análisis del riesgo desde el punto de vista de la seguridad?

B.3.3: Responsables y órganos para la gestión de cambios de aplicaciones o sistemas

- ¿Se han asignado responsabilidades para la gestión continuada de cambios en aplicaciones y sistemas?
- ¿Se han constituido organos para la gestión continuada de cambios en aplicaciones y sistemas?

B.3.4: Pruebas de testeo de los cambios en aplicaciones y sistemas

- ¿Se realizan pruebas de testeo de los cambios antes de la puesta en operación?
- ¿Qué tipo de pruebas se realizan?

B.3.5: Entornos para pruebas separados de producción

- ¿Se realizan pruebas de testeo de los cambios en entornos separados de la producción?

B.3.6: Aprobación del usuario en las pruebas de testeo

- ¿Se requiere de la aprobación del usuario para la aceptación de las pruebas de testeo previas a la puesta en operación?

B.3.7: Separación de las tareas para la gestión de cambios de aplicaciones o sistemas

- Las ejecución de las distintas acciones y responsabilidad en el proceso de gestión de cambios, ¿es realizada por distintas personas?
- ¿Se realiza el control de los accesos a los distintos entornos utilizado para desarrollo y pruebas de testeo en aplicaciones y sistemas de acuerdo a la separación de funciones implantada en el proceso de gestión de cambios?

B.3.8: Registro de cambios y solicitudes

- ¿Se realiza la gestión documental y el registro de las peticiones y los cambios en las aplicaciones y sistemas significativos?

Documentación necesaria:

- Copia del procedimiento de Gestión de Cambios
- Copia del procedimiento de procedimento de Gestión de la Configuración
- Copia de las actas de constitución de los organos de gestión de cambios
- Ejemplo de resultado de proceso completo de tramitación de un cambio de configuración de un sistema.
- Ejemplo de resultado de proceso completo de tramitación de un cambio de arquitectura o componente de un sistema.

C1 - CBCS 1: INVENTARIO DE DISPOSITIVOS AUTORIZADOS Y NO AUTORIZADOS

1-1: Inventario de activos físicos autorizados

- ¿Existe un inventario de hardware? En caso afirmativo:
  - ¿Proporciona información sobre los siguientes aspectos de cada elemento?
    - Identificación del activo: fabricante, modelo, número de serie
    - Configuración del activo: perfil, política, software instalado
    - Software instalado: fabricante, producto, versión y parches aplicados
    - Equipamiento de red: MAC, IP asignada (o rango)
    - Ubicación del activo: ¿dónde está?
    - Propiedad del activo: persona responsable del mismo
- ¿Está actualizado? Indicar la fecha de última actualización.
- ¿Dispone de una herramienta automatizada que permite la actualización continua del inventario? En caso afirmativo, indicar el nombre de la herramienta, fabricante y versión.
- Si no se dispone de herramienta, indicar cómo se lleva a cabo la actualización del inventario.
- ¿Dispone de un procedimiento de autorización de los elementos hardware antes de su entrada en producción? ¿Está aprobado? ¿Quién lo ha aprobado?

1-2: Control de activos físicos no autorizados

- ¿Dispone de mecanismos para controlar (detectar o restringir) el acceso de dispositivos físicos no autorizados (ej. 802.1x)?
- En caso contrario, ¿cómo garantiza que únicamente se conectan a la red los dispositivos autorizados?

Documentación necesaria:

- Copia del procedimiento de mantenimiento y gestión del inventario de hardware
- Copia del inventario de hardware
- Copia del procedimiento de autorización de hardware
- Copia del procedimiento donde se describan los controles para detectar o restringir el acceso de dispositivos físicos no autorizados.

C1 - CBCS 2: INVENTARIO DE SOFTWARE AUTORIZADO Y NO AUTORIZADO

2-1: Inventario de SW autorizado

- ¿Existe una lista actualizada de software autorizado?
- ¿Existe un inventario de software instalado en los dispositivos de la entidad?
  En caso afirmativo, ¿está actualizado? Indicar la fecha de última actualización.
- ¿Dispone de una herramienta automatizada para la gestión del inventario de software?
  En caso afirmativo, indicar el nombre de la herramienta, fabricante y versión.
- ¿El inventario de hardware y el de software están relacionados? (es decir, para un dispositivo hardware es posible consultar el software que tiene instalado).
- ¿Existe un procedimemiento de autorización de software?

2-2: SW soportado por el fabricante.

- ¿Dispone de un plan de mantenimiento del software, de acuerdo con las especificaciones de los fabricantes?
- El plan de mantenimiento anterior, ¿incluye el control de las fechas de fin de soporte del HW y SW por parte de los fabricantes?
- ¿Existe software fuera de soporte por parte del fabricante? En caso afirmativo, indicar producto, fabricante y versión.

2-3: Control de SW no autorizado

- ¿Se dispone de guías de instalación y bastionado de los sistemas previo a su entrada en operación?
- Las guías de configuración anteriores, ¿ incluyen el detalle del SW a instalar por tipo de sistema y/o usuario? (ej. SW a instalar en el equipo cliente de un usuario no administrador del área de gestión presupuestaria, SW a instalar en el servidor de BBDD de la aplicación X, etc.).
- ¿Dispone de alguna herramienta para controlar e impedir la instalación de software no autorizado (ej.applocker)? En caso afirmativo:
  - Indicar nombre de la herramienta, fabricante y versión.
  - ¿La herramienta detecta automáticamente el software instalado en cada sistema?¿Actualiza de forma automática el inventario de software?
- En caso contrario, ¿existe un procedimiento para la revisión del software instalado en los equipos de la entidad? En caso de detectar software no autorizado en estas revisiones, ¿se elimina?

Documentación necesaria:

- Copia del procedimiento de mantenimiento y gestión del inventario de software
- Copia del inventario de software
- Copia del procedimiento de autorización de software
- Copia del procedimiento/guías de configuración que indique los criterios para la instalación de software según el perfil de sistema y/o usuario.
- Copia del procedimiento de revisión del software instalado en los sistemas de la entidad.

C2 - CBCS 3: PROCESO CONTINUO DE IDENTIFICACIÓN Y REMEDIACIÓN DE VULNERABILIDADES

3-1 Identificación de vulnerabilidades

- ¿Se dispone de una herramienta para la identificación de las vulnerabilidades de seguridad que puedan afectar a los productos y tecnologías de sistemas de información existentes en la entidad?
- ¿Se efectúa un seguimiento continuo de los anuncios de defectos realizados por los fabricantes? ¿Cómo (ej. contratación de un servicio específico a fabricantes, suscripción a listas públicas de publicación de defectos, etc.)? ¿Quién es el responsable de realizarlo?
- Tras la puesta en servicio de un sistema, ¿se realizan análisis de vulnerabilidades periódicos?

3-2 Priorización de vulnerabilidades

- ¿Dispone de un procedimiento para analizar y priorizar la resolución de las vulnerabilidades y defectos de seguridad identificados, basado en la gestión de riesgos?
- ¿El procedimiento anterior define plazos máximos de resolución de las vulnerabilidades en función del riesgo asociado?

3-3 Resolución de vulnerabilidades

- ¿Se realiza el seguimiento de la corrección de las vulnerabilidades identificadas que, de acuerdo a la gestión de riesgos, se ha decidido resolver?

3-4 Parcheo

- ¿Se dispone de un procedimiento para el parcheo de sistemas/tecnologías (sistemas operativos, bases de datos, aplicaciones…)?
- ¿Se dispone de una/s herramienta/s para la gestión e instalación de parches y actualizaciones de seguridad? En caso afirmativo, indicar el nombre de la herramienta, fabricante y versión.

  En caso de utilizar herramientas diferentes en función de la tecnología, detallar de forma separada cada una de ellas.

Documentación necesaria:

- Copia del procedimiento (o procedimientos) de:
  - Identificación de vulnerabilidades.
  - Análisis y priorización de vulnerabilidades.
  - Seguimiento de la resolución de vulnerabilidades
  - Parcheo de sistemas/tecnologías.

C3 - CBCS 5: CONFIGURACIONES SEGURAS DE SOFTWARE Y HARDWARE EN DISPOSITIVOS MÓVILES, PORTÁTILES, EQUIPOS DE SOBREMESA Y SERVIDORES

5-1 Configuración segura

- ¿Dispone de un procedimiento de fortificación o bastionado de los sistemas previo a su entrada en operación?
- ¿Qué tipo de dispositivos cubre (servidores, equipos de sobremesa, portátiles, móviles y tabletas, etc.)?
- ¿Se utilizan imágenes o plantillas para aplicar la configuración de seguridad de todos los sistemas, de acuerdo con estándares aprobados por la organización?
- ¿Se realizan pruebas de seguridad antes de pasar a producción para comprobar que se cumplen los criterios en materia de seguridad?
- ¿Se dispone de alguna herramienta para realizar la tipología de pruebas anterior? En caso afirmativo, indicar nombre de la herramienta, fabricante y versión.
- Previo a la puesta en servicio de un nuevo sistema, aplicación, etc. ¿se realizan análisis de vulnerabilidades, pruebas de penetración y/o inspecciones de código fuente?

5-2: Gestión de la configuración

- Tras la puesta en producción de los sistemas, ¿se realizan comprobaciones periódicas para verificar que la configuración actual no ha sido modificada de forma no autorizada respecto de la configuración de seguridad original?
- ¿Se dispone de alguna herramienta para realizar la tarea anterior? En caso afirmativo, indicar nombre de la herramienta, fabricante y versión.
- ¿Se utilizan herramientas de configuración de los sistemas que impiden la modificación de la configuración de seguridad? En caso afirmativo, indicar nombre de la herramienta, fabricante y versión.
- ¿Se utiliza un sistema de supervisión de configuración para "monitorizar" en tiempo real la configuración de seguridad de todos sistemas de producción de la entidad? ¿La herramienta anterior permite definir alertas cuando se realizan cambios sobre dicha configuración?

  En caso afirmativo, indicar nombre de la herramienta, fabricante y versión.
- En caso de no disponer de herramientas que impidan o monitoricen la realización de cambios no autorizados en la configuración de seguridad de los sistemas ¿se dispone de otros mecanismos que garanticen lo anteior?

Documentación necesaria:

- Copia del procedimiento de pruebas de seguridad previas al pase a producción (en el que se detalle el alcance (qué sistemas deben pasar estas pruebas), responsables de definir las pruebas, ejecutarlas, aprobarlas, herramientas para realizarlas, etc.).
- Ejemplo del plan de pruebas de seguridad y resultado de su ejecución para un cambio realizado durante el año.
- Copia del procedimiento que regule la realización de análisis de vulnerabilidades, pruebas de penetración y/o inspección de código fuente previo al pase a producción.
- Ejemplo del resultado de un análisis de vulnerabilidades, una prueba de penetración y una inspección de código fuente realizados durante el ejercicio.

- Copia del procedimiento de gestión de la configuración (aquél que indique cómo garantizar que las configuraciones de seguridad no son modificadas de forma no autorizada tras la puesta en producción de un sistema.

C4 - CBCS 6: REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS (Mantenimiento, monitorización y análisis de los LOG de auditoría)

6-1: Activación de logs de auditoría (registro de la actividad de los usuarios)

- ¿Se registran las actividades de los usuarios en el sistema? En caso afirmativo indicar en qué sistemas (sistema operativo, bases de datos, aplicaciones) se encuentra activada.
- ¿El registro de auditoría indica quién realiza la actividad, cuándo la realiza y sobre qué información, sea cual sea el usuario?
- ¿Se han habilitado las opciones del registro de auditoría para que incluya información detallada, como direcciones de origen, direcciones de destino y otros datos útiles?
- ¿Incluye tanto las actividades realizadas con éxito como los intentos fracasados?

6-2: Almacenamiento de logs: Retención y protección

- ¿Dónde quedan almacenados los registros de actividad?
- ¿Se dispone de un inventario de los registros de actividad donde además se recoja el personal autorizado a su acceso, modificación o eliminación?
- ¿Qué mecanismos existen para proteger los registros de actividad frente a accesos y modificaciones o eliminación?
- ¿Está determinado el periodo de retención de los registros de actividad?
- ¿Se cuenta con un plan para garantizar la capacidad de almacenamiento de registros atendiendo a su volumen y política de retención?
- ¿Cómo se asegura que la fecha y hora de los mismos no puede ser manipulada?
- ¿Se realizan copias de seguridad de los registros de actividad?
- ¿Las copias de seguridad, si existen, se ajustan a los mismos requisitos?
- ¿Qué mecanismos existen para proteger las copias de seguridad de los registros de actividad frente a accesos y modificaciones o eliminación?

6-3: Centralización y revisión de los registros de la actividad de los usuarios

- ¿Se centralizan los logs generados en los diferentes sistemas?
- ¿Cómo? (volcado diario de los logs, reenvío de los logs al sistema central una vez escritos en el sistema original, escritura directa del log del sistema en el equipo centralizador de logs, etc.).
- ¿Se revisan los registros de actividad en busca de patrones anormales? En caso afirmativo, indicar alcance de las revisiones, responsables de su realización y periodicidad.

CBCS 6-4: Monitorización y correlación

- ¿Se dispone de alguna herramienta/utilidad que permita alertar, en tiempo real de sucesos anormales a partir del análisis de los logs de auditoría?

  En caso afirmativo, indicar nombre de la herramienta fabricante y versión.
- ¿La entidad dispone de un SIEM (Security Information and Event Management) o una herramienta de analítica de logs para realizar correlación y análisis de logs?

  En caso afirmativo, indicar nombre de la herramienta fabricante y versión.

Documentación necesaria:

- Copia de la política o normativa que establezca las directrices sobre el registro de actividades de los usuarios (qué se debe registrar, con qué detalle, de qué sistemas, periodo de retención, mecanismos de protección de los registros, etc.).
- Copia del inventario de los registros de actividad, donde además se recoja el personal autorizado a su acceso, modificación o eliminación.
- Copia del procedimiento en el que se establezca:
  - El periodo de retención de los registros de actividad y periodo de retención de evidencias tras un incidente.
  - Proceso para la eliminación de los registros tras el periodo estipulado de retención, incluyendo las copias de seguridad (si existen).
- Copia de la política de copia de seguridad de los registros de actividad (si se sigue una política específica para este tipo de información, no incluida en la política general de copia de seguridad de datos y sistemas (ver CBCS7)).
- Copia del procedimiento para la centralización de logs, en el que se indique las fuentes origen a centralizar, cómo se realizará la centralización, periodicidad, etc.
- Copia de una revisión de los registros de auditoría realizada durante el año y/o de los resultados obtenidos.

C.5: SERVICIOS EXTERNOS

C.5.1.- Nivel de Cumplimiento del Servicio

- ¿Dispone la entidad de un procedimiento de Contratación de Servicios Externos que documente los pasos previos a la contratación de servicios incluyendo el detalle por parte del proveedor de las características del servicio a prestar y los requisitos de servicio y seguridad requeridos?
- ¿Se incluye en los contratos firmados con el proveedor dichos acuerdos de nivel de servicio estipulados en el procedimiento de contratación?
- ¿Se detalla en el contrato las responsabilidades de ambas partes?
- ¿Se incluye en el contrato las consecuencias del incumplimiento de los acuerdos?

C.5.2.- Gestión del Nivel de Cumplimiento del Servicio

- ¿Se dispone de un sistema rutinario para medir el cumplimiento de las obligaciones de servicio?
- ¿Se han establecido mecanismos para la gestión de las desviaciones en indicadores incluidos en los acuerdos de nivel de servicio?
- ¿Se han establecido mecanismos para la gestión de incidentes durante el desempeño del servicio?

C.5.3.- Requisitos de Seguridad de los Servicios Externos

- ¿Se ha transmitido al proveedor de servicio sus obligaciones sobre la seguridad de los sistemas que proveen servicio a la administración mediante la inclusión de clausulas en los contratos?
- ¿Incluyen dichas clausulas las medidas de seguridad necesarias para el cumplimiento del ENS y son las incluidas en la Declaración de Aplicabilida?

C.5.4.- Gestión de la Seguridad de los Servicios de Cloud

- ¿Se ha transmitido al proveedor de servicio las obligaciones adicionales sobre la seguridad de los sistemas que proveen servicios de Cloud a la administración mediante la inclusión de clausulas en los contratos?
- ¿Se han incluido entre dichas obligaciones particulares las siguientes?:
    - Si los elementos de seguridad como Firewalls son virtualizados, no deben residir en las mismas máquinas que los componentes de producción.
    - El hypervisor se encuentra particularmente protegido mediante medidas adicionales a su nivel, particularmente en cuento a identificación, autenticación y autorización de administradores.
    - La red de gestión dedicada al servicio es distinta a otras redes de las que disponga el proveedor, incluyendo los equipos de conexión a internet para acceso remoto.
    - No se comparten equipos hypervisor para sistemas de distinta clasificación.
    - La adminsitración del hypervisor está diferenciada de la administración de los elementos virtualizados.

Documentación necesaria:

- Copia del procedimiento de Contratación de Servicios Externos
- Ejemplo de contrado de servicios externos.

C.6 PROTECCIÓN FRENTE A MALWARE

C.6.1.- Protección Frente a Código Dañino

- ¿Dispone de mecanismos de prevención y reacción frente a código dañino (virus, gusanos, troyanos, programas espía y "malware" en general)?
- ¿Sigue las directrices de configuración, mantenimiento y actualización del fabricante?
- ¿Qué mecanismos de actualización utiliza? ¿Con qué periodicidad? ¿Actualiza BBDD de Firmas? ¿Actualiza los puestos cliente?
- ¿Qué funcionalidades del producto tiene instaladas?
- ¿Cómo protege a aquello equipos que no pueden instalar el software de protección corporativo?

C.6.2.- Protección de Correo Electrónico

- ¿Se protege a la organización frente a problemas que se materializan por medio del correo electrónico como correo no deseado (spam)? ¿Qué mecanismos se utilizan?
- ¿Dispone la organización de herramientas para protegerse frente a código dañino en el Correo Electrónico?
- ¿Se ha establecido normativa de uso del Correo Electrónico y se ha comunicado a los usuarios?

Documentación necesaria:

- Copia del procedimiento de seguridad frente a código dañino o normativa específica

C.7 PROTECCIÓN DE INSTALACIONES E INFRAESTRUCTURA

C.7.1.- Control de Accesos a Instalaciones

- ¿Se dispone de distintas localizaciones para el equipamiento según su función?
- ¿Se controlan los accesos a dichos locales de acuerdo a una política de de identificación y autorización? ¿Qué métodos se utilizan?
- ¿Qué criterios se utilizan para proporcionar derechos de acceso?
- ¿Se registran los accesos?

C.7.2.- Infraestructura en CPD

- ¿Dispone el CPD y los centros de cableado de la infraestructura física necesaria para el cableado y la instalación de los sistemas?
- ¿Se dispone de canalizaciones independientes para energía y datos? ¿Se respetan las distancias mínimas?
- ¿Se dispone de falso suelo y/o techo en el CPD y los centros de cableado principales?

C.7.3.- Acondicionamiento de Locales

- ¿Los locales donde se ubican los sistemas de información y sus componentes disponen de sistemas para adecuar las condiciones de temperatura y humedad?
- ¿Se encuentran dichos sistemas dimensionados de acuerdo al consumo electrico y producción de calor actuales?
- ¿Se ha configurado el CPD considerando la óptima disipación del calor, por ejemplo mediante la impulsion de aire por suelo técnico y el uso de pasillos fríos y calientes?

C.7.4.- Suministro Eléctrico

- ¿Se garantiza el suministro de potencia eléctrica? ¿Se ha realizado un análisis de la potencia eléctrica necesaria?
- ¿Se garantiza la alimentación ininterrumpida ante fallo del suministro eléctrico mediante el uso de SAIS?
- ¿Se han dimensionado los SAIS para proporcionar a los sistemas críticos el tiempo suficiente para un apagado seguro?
- ¿Se proporciona el suministro eléctrico mediante acometidas redundantes? ¿Provienen de distintos cuadros eléctricos? ¿Provienen de distintos centros de transformación? (Control E3)
- ¿Existen métodos alternativos de suministro de energía en caso de fallo prolongado del servicio del proveedor? ¿Se dispone de grupo electrógeno fijo o móvil?

C.7.5.- Protección Frente a Incendios

- ¿Se dispone en CPDs y locales donde se ubican los sistemas de información de sistemas y medidas de protección frente a incendios? ¿Cuáles son?
- ¿Cumplen dichos sistemas con la normativa industrial existente?
- ¿Se encuentran dichos sistemas comunicados a centrales de alarmas?
- ¿Se ha considerado la protección pasiva contra incendios para el diseño de los elementos de CPD, tales como cubiertas de cableados, puertas o materiales de falso techo y suelo?

C.7.6.- Protección Frente a Inundaciones

- ¿Se protegen los locales donde se ubiquen los sistemas de información y sus componentes frente a incidentes fortuitos o deliberados causados por el agua?
- ¿Se utilizan sensores para la detección de humedad y agua en el CPD?
- ¿Se ha realizado el diseño del CPD y de los locales donde se ubican los sistemas de información de acuerdo a criterios para evitar el riesgo por causado por el agua?

Documentación necesaria:

- Documentación técnica de infraestructuras y elementos constructivos del CPD.
- Procedimiento de control de acceso físico a los locales donde se ubiquen los sistemas de información.

C.8 GESTIÓN DE INCIDENTES

C.8.1.- Detección de Incidentes y Eventos de los Sistemas

- ¿Se dispone de herramientas que permitan la gestión y detección temprana de incidentes de seguridad en los sistemas?
- ¿Se disponde de personal asignado al tratamiento de los eventos detectados?

C.8.2.- Gestión de Incidentes

- ¿Dispone de un proceso integral para hacer frente a incidentes que puedan tener un impacto en la seguridad del sistema?
- ¿Se encuentra dicho proceso plasmado en un procedimiento?
- ¿Incluye dicho procedimiento el escalado al responsable para la gestión del incidente?

C.8.3.- Respuesta ante Incidentes

- ¿Incluye la toma de medidas urgentes para la resolución del incidente?
- ¿Incluye la asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente?

C.8.4.- Comunicación de Incidentes

- ¿Incluye el procedimiento el proceso de notificación por parte del usuario o administrador del sistema que detecte el incidente?
- ¿Incluye el procedimiento la notificación al responsable para la gestión del incidente?
- ¿Incluye el procedimiento la notificación a las partes interesadas?

C.8.5.- Prevención de Incidentes y Mejora Continua

- ¿Incluye el procedimiento acciones para evitar la repetición de incidentes detectados?
- ¿Incluye el procedimiento un proceso de mejora continua para la optimización en la gestión de incidentes?

Documentación necesaria:

- Copia del procedimiento de Gestión de Incidentes

C.9 Monitorización

C.9.1.- Herramienta de monitorización de redes y sistemas

- ¿Se dispone de herramientas que permitan la monitorización del estado de redes y sistemas?
- ¿Se disponde de personal asignado a la monitorización del estado de los sistemas?

C.9.2.- Linea Base de los Sistemas

- ¿Proporciona la herramienta de monitorización información adecuada para establecer una línea base de utilización que puede ser explotada por equipo de TI?
- ¿Se utiliza la herramienta de monitorización para le detección de incidentes en base a comportamientos anómalos?
- ¿Se utiliza la herramiento de monitorización para la planificación estratégica y el dimensionamiento de nuevos sistemas de información?

C.9.3.- Registro de Eventos

- ¿Proporciona la herramienta información sobre los eventos detectados en las redes y sistemas?
- ¿Permite la herramienta la correlación de eventos para identificar causa raiz de incidentes?
- ¿Permite la herramienta la consulta de datos historicos para análisis forense de incidentes de seguridad?

Documentación necesaria:

- ¿?

D1 - CBCS 4: USO CONTROLADO DE PRIVILEGIOS ADMINISTRATIVOS

4-1 Inventario y control de cuentas de administración

- ¿Existe un procedimiento de gestión de privilegios que contemple la limitación de los privilegios de cada usuario al mínimo estrictamente necesario para acceder a la información requerida y para cumplir sus obligaciones?

  En particular, ¿el procedimiento anterior garantiza que se restringen los permisos de administración a los casos en que sea necesario y que sólo se utilicen las cuentas de administrador cuando sea necesario?
- ¿Se dispone de un inventario de las cuentas de administración que permita su adecuada gestión y control?
- ¿Los usuarios que no realizan funciones técnicas son administradores de sus equipos?

4-2 Cambio de contraseñas por defecto

- Antes de la puesta en producción de un sistema, ¿se eliminan/renombran las cuentas de administración estándar y se les cambia la contraseña por defecto?

4-3 Uso dedicado de cuentas de administración

- ¿Los usuarios que disponen de cuentas con plivilegios administrativos utilizan una cuenta nominativa sin privilegios de administrador para las tareas habituales y accesos a Internet o correo electrónico?
- Las cuentas de administración, ¿son nominativas? (es decir, cada usuario tiene la suya propia, no permitiendo el uso compartido de cuentas genéricas)

  En caso contrario, relacionar las cuentas de administración de uso compartido.
- Si existen cuentas de administración de uso compartido, ¿cómo se controla su uso? ¿cómo se gestiona la contraseña (distribución, cambio periódico, cambio tras cese de una de las personas que la conocían, etc.)?

4-4 Mecanismos de autenticación

- Para cada una de los sistemas / tecnologías existentes en la entidad, indicar el mecanismo de autenticación de las cuentas de administración.

  Si se utilizan contraseñas indicar las principales características de la política de autenticación (longitud mínima, vigencia máxima, vigencia mínima, requerimientos de complejidad (uso de mayúsculas, minúsculas, números y caracteres especiales), histórico de contraseñas recordadas).

Sistema / Tecnología	Mecanismo de autenticación	Características principales
Ej: SGBD Oracle 11.2	Contraseña	….
Ej:Aplicación XXXXX	Certificado + contraseña	….
Dominio Windows (servidores y equipos de usuario)	Certificado + contraseña	

- ¿Se dispone de un procedimiento para regular la gestión de las cuentas de administración? (ej. construcción del identificador de usuario, distribución de la contraseña/credencial, etc.)

- El procedimiento anterior ¿contempla el que se retiren/deshabiliten/eliminen las cuentas de administración cuando la persona termina su relación con la entidad?

4-5 Auditoría y control del uso de las cuentas con privilegios de administración

- Se dispone de un registro de actividad de las acciones realizadas con cuentas y sobre cuentas de administración para todos los sistemas (sistemas operativos, bases de datos, aplicaciones, etc.) de la entidad?
- ¿Contempla el registro tanto de acciones exitosas como fallidas?
- ¿Existe algún sistema en el que el registro anterior no esté habilitado? En caso afirmativo, indicar cuál.
- ¿Existen alertas automáticas cuando se asignan/desasignan privilegios de administración? ¿Quién las recibe y las aprueba en su caso?
- ¿Existen alertas automáticas cuando se supera un umbral de intentos de acceso fallidos mediante una cuenta con privilegios de administración?
- ¿Qué mecanismos se utilizan para evitar que los propios administradores de los sistemas modifiquen los registros de auditoría de las acciones realizadas con cuentas de administración?

Documentación necesaria:

- Copia del procedimiento de gestión de privilegios (en particular, privilegios de administración)
- Copia del procedimiento de inventariado de cuentas de administración
- Copia del inventario de cuentas de administración
- Copia del procedimiento de instalación/bastionado de sistemas, o aquél que contemple el control de renombrado/eliminación de cuentas estándar con privilegios de administración y las correspondientes contraseñas
- Copia del procedimiento de gestión de cuentas de administración (ej. construcción del identificador de usuario, distribución de la contraseña/credencial, etc.)

Copia del procedimiento para el registro de las acciones realizadas con cuentas de administración.

D.2 MECANISMOS DE IDENTIFICACIÓN Y AUTENTICACIÓN

D.2.1.- Procedimiento de Identificación y Autenticación de Usuarios

- ¿Se dispone de un procedimiento de gestión que contemple los mecanismos utilizados para la identificación y autenticación de los usuarios?

D.2.2.- Identificación de Usuarios

- ¿Se dispone de identificadores singulares de usuario para el acceso a los sistemas?
- ¿Cada usuario que accede al sistema tiene asignado distintos identificadores únicos en función de cada uno de los roles que deba desempeñar en el sistema?
- ¿Se inhabilita el identificador cuando el usuario deja la organización, 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?
- Si el identificador debe ser eliminado, ¿se mantiene durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas?

D.2.3.- Auntenticación de Usuarios

- ¿Cuál es el mecanismo de autenticación de los sistemas según su nivel?
- ¿El algoritmo de autenticación está acreditado o certificado?
- ¿Se ha implantado una política de contraseñas que fije la calidad mínima y el periodo para la renovación de la misma?
- ¿Se utiliza doble factor de autenticación en algún caso?
- ¿Se retiran y deshabilitan las credenciales cuando el usuario que autentican termina su relación con el sistema?
- ¿Se suspenden las credenciales tras un periodo definido de no utilización?

Documentación necesaria:

- Procedimiento de Gestión de Usuarios /Identificación /Autenticación /Gestión de Contraseñas/ Gestión de Derechos de Acceso

D.3 GESTIÓN DE DERECHOS DE ACCESO

D.3.1.- Procedimiento de Gestión de Derechos de Acceso

- ¿Se dispone de un procedimiento de gestión que contemple la mecanismos utilizados para el control de los derechos de acceso de los usuarios a los sistemas?

D.3.2.- Mecanismos de Control de los Accesos

- ¿Cuentan los sistemas críticos con mecanismos de control de accesos que impidan la utilización de sus recursos?
- ¿Se establecen los derechos de acceso de cada recurso según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema?
- Los mecanismo de control de accesos, ¿incluyen la distinción en el acceso a los distintos recursos del sistema y a los ficheros de configuración?
- ¿Se registran los accesos con éxito y los fallidos?
- ¿Se limita el número de intentos fallidos de acceso?.
- ¿Informa el sistema al usuario de sus obligaciones para obtener el acceso?
- ¿Se limita el horario, fechas y lugar desde donde se accede?
- ¿Se han establecido puntos en los que el sistema requerirá una renovación de la autenticación del usuario?

D.3.3.- Principio para la Asignación de Derechos de Acceso

- ¿Se limitan los privilegios de cada usuario al mínimo estrictamente necesario para acceder a la información requerida y para cumplir sus obligaciones?
- ¿Puede sólo y exclusivamente el personal con competencia para ello conceder, alterar o anular la autorización de acceso a los recursos conforme a los criterios establecidos por su responsable?

Documentación necesaria:

- Procedimiento de Gestión de Usuarios /Identificación /Autenticación /Gestión de Contraseñas/ Gestión de Derechos de Acceso

D.4 GESTIÓN DE USUARIOS

D.4.1.- Procedimiento de Gestión de Usuarios

- ¿Se dispone de un procedimiento de gestión de los usuarios de los sistemas?

D.4.2.- Definición de Puestos de Trabajo

- ¿Se ha caracterizado cada puesto de trabajo?
- ¿Incluye dicha caracterización la definición de las responsabilidades relacionadas con el puesto de trabajo?
- ¿Incluye dicha caracterización la definición de los derechos de acceso sobrte los sistemas?

D.4.3.- Gestión Continuada de los Derechos de los Usuarios

- ¿Realiza la entidad la gestión de los usuarios del sistema y sus privilegios de acuerdo a sus obligaciones y responsabilidades?
- ¿Revisa periodicamente la actividad de los usuarios para identificar los usuarios inactivos?
- ¿Revisa periodicamente las bajas en la entidad y las diferencias con los usuarios activos?

Documentación necesaria:

- Procedimiento de Gestión de Usuarios /Identificación /Autenticación /Gestión de Contraseñas/ Gestión de Derechos de Acceso

D.5 PROTECCIÓN DE REDES y COMUNICACIONES

D.5.1.- Protección por Firewall

- ¿Dispone de dispositivo Firewall que realice funciones de control de acceso exterior?
- ¿Dispone el Firewall de alguna de las siguientes funcionalidades avanzadas?:
    - IDS
    - IPS
    - DPI (Deep Packet Inspection)
    - Application Inspection
    - DLP (Data Leak Prevention)
    - Inspección de tráfico encriptado
- ¿Se mantiene adecuadamente actualizado el firewall en cuanto a firmas y otra información de terceros para el procesado de seguridad?

D.5.2.- Arquitectura de Red

- ¿Se ha realizado un diseño considerando el uso de DMZ para alojar a los elementos que requieren comunicación con el exterior?
- En caso de existir DMZ, ¿son los firewalls internos y externos de distintos fabricantes?
- ¿Disponen los sistemas de Firewall de la adecuada redundancia hardware?

D.5.3.- Conexiones Exteriores Seguras

- ¿Se emplean redes privadas virtuales (VPN) cuando la comunicación discurre por redes fuera del propio dominio de seguridad?
- ¿Utilizan dichas conexiones privadas vistuales algoritmos acreditados por el CCN?

D.5.4.- Segmentación de Redes

- ¿Se encuentra la red segmentada?
- ¿Qué criterio se utiliza para el diseño y dimensionamiento de la segmentación?
- ¿Cuál es el tamaño máximo por segmento?
- ¿Se encuentra el dispositivo de interconexión (Firewall, Router) entre segmentos particularmente monitorizado y protegido?

D.5.5.- Mecanismos de Identificación y Autenticación para Gestión de Red

- ¿Se utilizan configuraciones seguras para la identificación y autenticación de administradores de los sistemas de comunicaciones y electrónica de red?
- ¿Se utilizan conexiones seguras como SSH? ¿Se ha deshabilitado el acceso por telnet?
- ¿Se han implementado mecanismos de encriptación de contraseñas en la configuración de los equipos de comunicaciones?
- ¿Se han implementado mecanismos de autenticación basados en el uso de servidores de autenticación, utilizando protocolos de autenticación como RADIUS o TACACS?

D.5.6.- Gestión segura de Logs y Notificaciones

- ¿Se implementan configuraciones seguras para gestionar los eventos y notificaciones del los sistemas de comunicaciones?
- ¿Se utilizan repositorios externos para la recepción y tratamientyo de las notificaciones generadas por los equipos de comunicaciones y electrónica de red?
- ¿Se utilizan protocolos seguros para la comunicación de eventos y notificaciones? ¿Se utiliza SNMPv3 y se ha deshabilitado el uso de protocolos obsoletos como SNMPv1 o SNMPv2?

D.5.7.- Configuraciones por Defecto y Automáticas

- ¿Se utiliza en el equipamiento de comunicaciones y electrónica de red configuraciones automáticas?
- ¿Se utiliza configuración dinámica de trunks?
- ¿Se utiliza configuración dinámica de vlans?
- ¿Se utiliza configuración dinámica de Etherchannels?
- ¿Se utilizan en el equipamiento de comunicaciones y electrónica de red configuraciones por defecto?
- ¿Se encuentra la vlan 1 utilizada en la electrónica de red?
- ¿Se mantienen habilitados por defecto los puertos de la electrónica de red?
- ¿Se ha deshabilitado el servidor web embebido en los dispositivos de electrónica de red?
- ¿Se encuentra deshabilitada La conexión a la electrónica de red mediante protocolo telnet?
- ¿Se encuentra deshabilitado El servidor FTP embebido en la electrónica de red?
- ¿Se han modificado la comunity string por defecto de SNMPv1 y v2?
- ¿Se ha dehabilitado el uso de versiones anteriores a SNMPv3?
- ¿Se ha modificado el prompt por defecto?

D.5.8.- Mecanismos contra Ataques LAN

- ¿Se utilizan mecanismos de seguridad para evitar ataques en la red de área local? ¿Cuales son dichos mecanismos?

D.5.9.- Control de Acceso a los Recursos de Red

- ¿Se utilizan mecanismos para limitar el acceso a recursos de la red? ¿Cuales son dichos mecanismos?
- ¿Se utiliza 802.1x para el control perimetral?
- ¿Se protegen las comunicaciones para la gestión de routing dinámico (si se emplea) mediante mecanismos de acutenticación?
- ¿Se protegen las comunicaciones de los protocolos de alta disponibilidad?

Documentación necesaria:

- ¿?

E1 - CBCS 7 Copia de seguridad de datos y sistemas

7.1.- Copia de seguridad de datos y sistemas

- ¿Se realizan copias de respaldo que permitan recuperar datos perdidos con una antigüedad determinada?

En cuanto a la política de copia de seguridad:

  - ¿Incluye datos (información de trabajo) de la entidad?
  - ¿Algún sistema, conjunto de datos, etc. queda fuera del alcance de la política de copia?
  - ¿Abarca los datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga?
  - Si se utiliza criptografía para el cifrado de la información, ¿la política de copia incluye el respaldo de las claves criptográficas?
  - Indicar tipo de copia y periodicidad (ej. Incremental diaria, completa semanal, etc.).
  - ¿Se dispone de herramienta/s para la realización de copias de seguridad? En caso afirmativo, indicar el nombre de la herramienta, fabricante y versión.
  - ¿En qué soporte se almacenan las copias de seguridad realizadas?
  - ¿Se externalizan las copias de seguridad? ¿Dónde? (ej. a un edificio distinto, a una sala distinta dentro del mismo edificio, a las instalaciones de un proveedor, etc.)
  - Se utilizan servicios en la nube para el almacenamiento de backups? En caso afirmativo, indicar qué servicio se utiliza y el proveedor que lo presta.

7.2.- Pruebas de recuperación

- ¿Se realizan pruebas de recuperación a partir de las copias de respaldo realizadas?
  - Indicar alcance de las pruebas de recuperación y periodicidad.
  - ¿Se documentan (o queda algún registro) de la realización de dichas pruebas de recuperación y las incidencias identificadas?

7.3.- Protección de los backups

- ¿Los backups disfrutan de la misma seguridad que los datos originales, tanto en su acceso, almacenamiento como transporte?

  Indicar brevemente los mecanismos utilizados para dicho propósito.
- En cuanto a solicitudes puntuales de recuperación de datos por parte de los usuarios de la organización, ¿se dispone de un procedimiento que establezca cómo debe realizarse (quién puede solicitar, cómo, quién debe autorizar, etc.)?
- ¿Las copias de seguridad están accesibles de forma directa a nivel de red?
- ¿Se dispone de una copia de seguridad en un soporte desconectado de la red? ¿Cómo y con qué frecuencia se realiza?

Documentación necesaria:

- Copia del procedimiento de copia de seguridad de datos y sistemas
- Copia del procedimiento de restauración a partir de las copias de seguridad realizadas
- Copia de los informes, registros, etc. de las pruebas de recuperación realizadas en el último año

- Copia del procedimiento para la solicitud de recuperaciones puntuales de información a partir de las copias de seguridad realizadas

E.2 PLAN DE CONTINUIDAD

E.2.1.- Identificación de Elementos Críticos de la Actividad

- ¿Se ha realizado un Análisis de Impacto en la Actividad para identificar los servicios críticos?
- ¿Se han identificado los requisitos de disponibilidad de los servicios?
- ¿Se han identificado los sistemas y elementos que sustenan los servicios críticos?

E.2.2.- Plan de Continuidad de la Actividad

- ¿Dispone de un Plan de Continuidad de la Actividad?
- ¿Identifica los roles, sus responsabilidades y las funciones a realizaren caso de crisis?
- ¿Existe una previsión de medios alternativos para permitir la continuidad del servicio?
- ¿Ha recibido el personal involucrado en el PCN la formación necesaria para ejercitar sus funciones?
- ¿Es parte de otros planes de la entidad que trascienden de los Sistemas de Información y su seguridad?

E.2.3.- Pruebas del Plan de Continuidad de la Actividad

- ¿Se realizan pruebas periódicas para localizar y corregir, en su caso, los errores o deficiencias que puedan existir en el plan de continuidad?
- ¿Con qué periodicidad se realizan?
- ¿Se lleva a cabo la totalidad de las acciones del Plan o se limita el alcance en cada prueba?

Documentación necesaria:

- Plan de Continuida de la Actividad / Plan de Recuperación de Desastres
- Análisis de Impacto en la Actividad

E.3 ALTA DISPONIBILIDAD

E.2.1.- Diseño enfocado a la Alta Disponibilidad

- ¿Se considera la Alta Disponibilidad como criterio en el diseño, adquisición y desarrollo de los sistemas?

E.2.2.- Ubicaciones Redundantes

- ¿Se dispone de ubicaciones redundantes para los locales de que albergan sistemas de información o elementos crítiticos de los mismos?
- ¿Dispone de CPD redundado?
- ¿Se encuentran redundados los centros de cableado principales?

E.2.3.- Elementos Redundantes de Sistemas Críticos

- ¿Dispone de redundancia eléctrica en los locales que albergan sistemas de información?
- ¿Se encuentran redundados y discurren por caminos y canalizaciones independientes los enlaces de comunicaciones que proporcionan servicio a elementos críticos de la red?
- ¿Se encuentran redundados los equipos de comunicaciones que realizan tareas críticas en la red.
- ¿Disponen de doble fuente de alimentaciónlos equipos de comunicaciones que realizan tareas críticas en la red?
- ¿Disponen de doble tarjeta supervisora los equipos de comunicaciones que realizan tareas críticas en la red?
- ¿Se encuntran redundados en localizaciones distintas los servidores que realizan tareas críticas o albergan la ejecución de aplicaciones críticas?
- ¿Disponen de doble fuente de alimentación los servidores que realizan tareas críticas o albergan la ejecución de aplicaciones críticas?

Documentación necesaria:

- Copia del procedimiento o metodología utilizada para el desarrollo de sistemas y aplicaciones.
- Copia del documento de arquitectura básica de los sistemas