INSTRUCIÓNS:

O seguinte cuestionario pretende articular o alcance da revisión preliminar sobre os controis máis directamente relacionados coa ciberseguridade e cumprimento da legalidade nos sistemas de información da entidade, enmarcado dentro das actividades de planificación da auditoría que se está levando a cabo.

Para cumprimentar o cuestionario non é necesario que se xere documentación adicional á xa dispoñible. A idea é a de dispoñer da documentación xa existente na entidade no momento de inicio do traballo de campo, co fin de optimizar o tempo investido por ambas partes.

O traballo de campo desenvolverase principalmente mediante entrevistas, das que poderán xurdir necesidades adicionais de información.

No caso de que exista documentación descritiva dos procedementos, non é necesaria a cumprimentación do cuestionario respecto a eses aspectos, basta coa achega do documento descritivo.

Do mesmo xeito, non é imprescindible que nos facilite aquela información que considere pode ser de carácter confidencial. Neses casos indíqueo no cuestionario e prepárea para o inicio do traballo.

O alcance da revisión posúe un carácter xeral, non sendo necesario obter unha información exhaustiva de cada un dos puntos incluídos no cuestionario.

Para calquera dúbida, non dubide en poñerse en contacto cos membros do equipo de fiscalización (Correo electrónico: XXX@xx.xx, tf. xxx).

Rogámoslle nos facilite o cuestionario cumprimentado canto antes.

Unha vez cumprimentado devolverase como un documento ***.docx o *.pdf asinado electronicamente (preferentemente) ou en soporte papel con firma hológrafa da responsable da área de sistemas de información.**

CUMPRIMENTADO POR:

Entidade:

Denominación do Departamento TI:

Nome:

Cargo:

Data:

Sinatura:

Domicilio do Departamento TI:

INFORMACIÓN XERAL SOBRE A CONTORNA TECNOLÓXICA DA ENTIDADE

Documentación necesaria:

- Copia do mapa de rede
- Diagramas da arquitectura física/lóxica dos sistemas de información da Entidade

En caso de non dispoñer de dita documentación, incluír unha breve explicación da contorna de TI da Entidade (existencia ou non de DMZ, de segmentación entre rede de usuarios e rede de servidores, elementos de seguridade (firewall, IPS, etc.), relación dos principais sistemas situados na rede interna, uso de solucións de virtualización, etc.).

CBCS 1: INVENTARIO DE DISPOSITIVOS AUTORIZADOS E NON AUTORIZADOS

1-1: Inventario de activos físicos autorizados

- Existe un inventario de hardware? En caso afirmativo:
  - Proporciona información sobre os seguintes aspectos de cada elemento?
    - Identificación do activo: fabricante, modelo, número de serie
    - Configuración do activo: perfil, política, software instalado
    - Software instalado: fabricante, produto, versión e parches aplicados
    - Equipamento de rede: MAC, IP asignada (ou rango)
    - Localización do activo: onde está?
    - Propiedade do activo: persoa responsable do mesmo
- Está actualizado? Indicar a data de última actualización.
- Dispón dunha ferramenta automatizada que permite a actualización continua do inventario? En caso afirmativo, indicar o nome da ferramenta, fabricante e versión.
- Se non se dispón de ferramenta, indicar como leva a cabo a actualización do inventario.
- Dispón dun procedemento de autorización dos elementos hardware antes da súa entrada en produción? Está aprobado? Quen o aprobou?

1-2: Control de activos físicos non autorizados

- Dispón de mecanismos para controlar (detectar ou restrinxir) o acceso de dispositivos físicos non autorizados (ex. 802.1x)?
- En caso contrario, como garante que unicamente se conectan á rede os dispositivos autorizados?

Documentación necesaria:

- Copia do procedemento de mantemento e xestión do inventario de hardware
- Copia do inventario de hardware
- Copia do procedemento de autorización de hardware
- Copia do procedemento onde se describan os controis para detectar ou restrinxir o acceso de dispositivos físicos non autorizados.

CBCS 2: INVENTARIO DE SOFTWARE AUTORIZADO E NON AUTORIZADO

2-1: Inventario de SW autorizado

- Existe unha lista actualizada de software autorizado?
- Existe un inventario de software instalado nos dispositivos da entidade?

  En caso afirmativo, está actualizado? Indicar a data de última actualización.
- Dispón dunha ferramenta automatizada para a xestión do inventario de software?

  En caso afirmativo, indicar o nome da ferramenta, fabricante e versión.
- O inventario de hardware e o de software están relacionados? (é dicir, para un dispositivo hardware é posible consultar o software que ten instalado).
- Existe un procedemento de autorización de software?

2-2: SW soportado polo fabricante.

- Dispón dun plan de mantemento do software, de acordo coas especificacións dos fabricantes?
- O plan de mantemento anterior, inclúe o control das datas de fin de soporte do HW e SW por parte dos fabricantes?
- Existe software fóra de soporte por parte do fabricante? En caso afirmativo, indicar produto, fabricante e versión.

2-3: Control de SW non autorizado

- Disponse de guías de instalación e bastionado dos sistemas previo á súa entrada en operación?
- As guías de configuración anteriores, inclúen o detalle do SW a instalar por tipo de sistema e/ou usuario? (ex. SW a instalar no equipo cliente dun usuario non administrador da área de xestión orzamentaria, SW a instalar no servidor de BBDD da aplicación X, etc.).
- Dispón dalgunha ferramenta para controlar e impedir a instalación de software non autorizado (ej.applocker)? En caso afirmativo:
  - Indicar nome da ferramenta, fabricante e versión.
  - A ferramenta detecta automaticamente o software instalado en cada sistema? Actualiza de forma automática o inventario de software?
- En caso contrario, existe un procedemento para a revisión do software instalado nos equipos da entidade? En caso de detectar software non autorizado nestas revisións, elimínase?

Documentación necesaria:

- Copia do procedemento de mantemento e xestión do inventario de software.
- Copia do inventario de software.
- Copia do procedemento de autorización de software.
- Copia do procedemento/guías de configuración que indique os criterios para a instalación de software segundo o perfil de sistema e/ou usuario.
- Copia do procedemento de revisión do software instalado nos sistemas da entidade.

CBCS 3: PROCESO CONTINUO DE IDENTIFICACIÓN E REMEDIACIÓN DE VULNERABILIDADES

3-1 Identificación de vulnerabilidades

- Disponse dunha ferramenta para a identificación das vulnerabilidades de seguridade que poidan afectar os produtos e tecnoloxías de sistemas de información existentes na entidade?
- Efectúase un seguimento continuo dos anuncios de defectos realizados polos fabricantes? Como (ex. contratación dun servizo específico a fabricantes, subscrición a listas públicas de publicación de defectos, etc.)? Quen é o responsable de realizalo?
- Tras a posta en servizo dun sistema, realízanse análise de vulnerabilidades periódicos?

3-2 Priorización de vulnerabilidades

- Dispón dun procedemento para analizar e priorizar a resolución das vulnerabilidades e defectos de seguridade identificados, baseado na xestión de riscos?
- O procedemento anterior define prazos máximos de resolución das vulnerabilidades en función do risco asociado?

3-3 Resolución de vulnerabilidades

- Realízase o seguimento da corrección das vulnerabilidades identificadas que, de acordo á xestión de riscos, decidiuse resolver?

3-4 Parcheo

- Disponse dun procedemento para o parcheo de sistemas /tecnoloxías (sistemas operativos, bases de datos, aplicacións…)?
- Disponse dunha/s ferramenta/s para a xestión e instalación de parches e actualizacións de seguridade? En caso afirmativo, indicar o nome da ferramenta, fabricante e versión.

  En caso de utilizar ferramentas diferentes en función da tecnoloxía, detallar de forma separada cada unha delas.

Documentación necesaria:

- Copia do procedemento (ou procedementos) de :
  - Identificación de vulnerabilidades.
  - Análise e priorización de vulnerabilidades.
  - Seguimento da resolución de vulnerabilidades
  - Parcheo de sistemas/tecnoloxías.

CBCS 4: USO CONTROLADO DE PRIVILEXIOS ADMINISTRATIVOS

4-1 Inventario e control de contas de administración

- Existe un procedemento de xestión de privilexios que contemple a limitación dos privilexios de cada usuario ao mínimo estritamente necesario para acceder á información requirida e para cumprir as súas obrigas?

  En particular, o procedemento anterior garante que se restrinxen os permisos de administración aos casos en que sexa necesario e que só se utilicen as contas de administrador cando sexa necesario?
- Dispone dun inventario das contas de administración que permita a súa adecuada xestión e control?
- Os usuarios que non realizan funcións técnicas son administradores dos seus equipos?

4-2 Cambio de contrasinais por defecto

- Antes da posta en produción dun sistema, elimínanse/renomeanse as contas de administración estándar e cámbiaselles o contrasinal por defecto?

4-3 Uso dedicado de contas de administración

- Os usuarios que dispoñen de contas con plivilexios administrativos utilizan unha conta nominativa sen privilexios de administrador para as tarefas habituais e accesos a Internet ou correo electrónico?
- As contas de administración, son nominativas? (é dicir, cada usuario ten a súa propia, non permitindo o uso compartido de contas xenéricas)

  En caso contrario, relacionar as contas de administración de uso compartido.
- Se existen contas de administración de uso compartido, como se controla o seu uso? como se xestiona o contrasinal (distribución, cambio periódico, cambio tras cesamento dunha das persoas que a coñecían, etc.)?

4-4 Mecanismos de autenticación

- Para cada unha dos sistemas / tecnoloxías existentes na entidade, indicar o mecanismo de autenticación das contas de administración.

  Se se utilizan contrasinais indicar as principais características da política de autenticación (lonxitude mínima, vixencia máxima, vixencia mínima, requirimentos de complexidade (uso de maiúsculas, minúsculas, números e caracteres especiais), histórico de contrasinais lembrados).

Sistema / Tecnoloxía	Mecanismo de autenticación	Características principais
Ej: SGBD Oracle 11.2	Contrasinal	….
Ej:Aplicación XXXXX	Certificado + contrasinal	….
Dominio Windows (servidores e equipos de usuario)	Certificado + contrasinal	

- Dispone dun procedemento para regular a xestión das contas de administración? (ex. construción do identificador de usuario, distribución do contrasinal/credencial, etc.)
- O procedemento anterior contempla o que se retiren/deshabiliten/eliminen as contas de administración cando a persoa termina a súa relación coa entidade?

4-5 Auditoría e control do uso das contas con privilexios de administración

- Disponse dun rexistro de actividade das accións realizadas con contas e sobre contas de administración para todos os sistemas (sistemas operativos, bases de datos, aplicacións, etc.) da entidade?
- Contempla o rexistro tanto de accións exitosas como erradas?
- Existe algún sistema no que o rexistro anterior non estea habilitado? En caso afirmativo, indicar cal.
- Existen alertas automáticas cando se asignan/desasignan privilexios de administración? Quen as recibe e as aproba no seu caso?
- Existen alertas automáticas cando se supera un limiar de intentos de acceso errados mediante unha conta con privilexios de administración?
- Que mecanismos se utilizan para evitar que os propios administradores dos sistemas modifiquen os rexistros de auditoría das accións realizadas con contas de administración?

Documentación necesaria:

- Copia do procedemento de xestión de privilexios (en particular, privilexios de administración)
- Copia do procedemento de inventariado de contas de administración
- Copia do inventario de contas de administración
- Copia do procedemento de instalación/bastionado de sistemas, ou aquel que contemple o control de renomeado/eliminación de contas estándar con privilexios de administración e os correspondentes contrasinais
- Copia do procedemento de xestión de contas de administración (ex. construción do identificador de usuario, distribución do contrasinal/credencial, etc.)
- Copia do procedemento para o rexistro das accións realizadas con contas de administración.

CBCS 5: CONFIGURACIÓNS SEGURAS DE SOFTWARE E HARDWARE EN DISPOSITIVOS MÓBILES, PORTÁTILES, EQUIPOS DE SOBREMESA E SERVIDORES

5-1 Configuración segura

- Dispón dun procedemento de fortificación ou bastionado dos sistemas previo á súa entrada en operación?
- Que tipo de dispositivos cobre (servidores, equipos de sobremesa, portátiles, móbiles e tabletas, etc.)?
- Utilízanse imaxes ou patróns para aplicar a configuración de seguridade de todos os sistemas, de acordo con estándares aprobados pola organización?
- Realízanse probas de seguridade antes de pasar a produción para comprobar que se cumpren os criterios en materia de seguridade?
- Disponse dalgunha ferramenta para realizar a tipoloxía de probas anterior? En caso afirmativo, indicar nome da ferramenta, fabricante e versión.
- Previo á posta en servizo dun novo sistema, aplicación, etc. realízanse análises de vulnerabilidades, probas de penetración e/ou inspeccións de código fonte?

CBCS 5-2: Xestión da configuración

- Tras a posta en produción dos sistemas, realízanse comprobacións periódicas para verificar que a configuración actual non foi modificada de forma non autorizada respecto da configuración de seguridade orixinal?
- Disponse dalgunha ferramenta para realizar a tarefa anterior? En caso afirmativo, indicar nome da ferramenta, fabricante e versión.
- Utilízanse ferramentas de configuración dos sistemas que impiden a modificación da configuración de seguridade? En caso afirmativo, indicar nome da ferramenta, fabricante e versión.
- Utilízase un sistema de supervisión de configuración para "monitorar" en tempo real a configuración de seguridade de todos os sistemas de produción da entidade? A ferramenta anterior permite definir alertas cando se realizan cambios sobre dita configuración?

  En caso afirmativo, indicar nome da ferramenta, fabricante e versión.
- En caso de non dispoñer de ferramentas que impidan ou monitoren a realización de cambios non autorizados na configuración de seguridade dos sistemas disponse doutros mecanismos que garantan o anterior?

Documentación necesaria:

- Copia do procedemento de probas de seguridade previas ao pase a produción (no que se detalle o alcance (que sistemas deben pasar estas probas), responsables de definir as probas, executalas, aprobalas, ferramentas para realizalas, etc.).
- Exemplo do plan de probas de seguridade e resultado da súa execución para un cambio realizado durante o ano.
- Copia do procedemento que regule a realización de análise de vulnerabilidades, probas de penetración e/ou inspección de código fonte previo ao pase a produción.
- Exemplo do resultado dunha análise de vulnerabilidades, unha proba de penetración e unha inspección de código fonte realizados durante o exercicio.
- Copia do procedemento de xestión da configuración (aquel que indique como garantir que as configuracións de seguridade non son modificadas de forma non autorizada tras a posta en produción dun sistema.

CBCS 6: REXISTRO DA ACTIVIDADE DOS USUARIOS (Mantemento, monitorización e análise dos LOG de auditoría)

6-1: Activación de logs de auditoría (rexistro da actividade dos usuarios)

- Rexístranse as actividades dos usuarios no sistema? En caso afirmativo indicar en que sistemas (sistema operativo, bases de datos, aplicacións) atópase activada.
- O rexistro de auditoría indica quen realiza a actividade, cando a realiza e sobre que información, sexa cal for o usuario?
- Habilitáronse as opcións do rexistro de auditoría para que inclúa información detallada, como direccións de orixe, direccións de destino e outros datos útiles?
- Inclúe tanto as actividades realizadas con éxito como os intentos fracasados?

6-2: Almacenamento de logs: Retención e protección

- Onde quedan almacenados os rexistros de actividade?
- Disponse dun inventario dos rexistros de actividade onde ademais se recolla o persoal autorizado ao seu acceso, modificación ou eliminación?
- Que mecanismos existen para protexer os rexistros de actividade fronte a accesos e modificacións ou eliminación?
- Está determinado o período de retención dos rexistros de actividade?
- Cóntase cun plan para garantir a capacidade de almacenamento de rexistros atendendo ao seu volume e política de retención?
- Como se asegura que a data e hora dos mesmos non pode ser manipulada?
- Realízanse copias de seguridade dos rexistros de actividade?
- As copias de seguridade, se existen, axústanse aos mesmos requisitos?
- Que mecanismos existen para protexer as copias de seguridade dos rexistros de actividade fronte a accesos e modificacións ou eliminación?

6-3: Centralización e revisión dos rexistros da actividade dos usuarios

- Centralízanse os logs xerados nos diferentes sistemas?
- Como? (envorcado diario dos logs, reenvío dos logs ao sistema central unha vez escritos no sistema orixinal, escritura directa do log do sistema no equipo centralizador de logs, etc.).
- Revísanse os rexistros de actividade en busca de patróns anormais? En caso afirmativo, indicar alcance das revisións, responsables da súa realización e periodicidade.

CBCS 6-4: Monitorización e correlación

- Disponse dalgunha ferramenta/utilidade que permita alertar, en tempo real de sucesos anormais a partir da análise dos logs de auditoría?

  En caso afirmativo, indicar nome da ferramenta fabricante e versión.
- A entidade dispón dun SIEM (Security Information and Event Management) ou unha ferramenta de analítica de logs para realizar correlación e análise de logs?

  En caso afirmativo, indicar nome da ferramenta fabricante e versión.

Documentación necesaria:

- Copia da política ou normativa que estableza as directrices sobre o rexistro de actividades dos usuarios (que se debe rexistrar, con que detalle, de que sistemas, período de retención, mecanismos de protección dos rexistros, etc.).

- Copia do inventario dos rexistros de actividade, onde ademais se recolla o persoal autorizado ao seu acceso, modificación ou eliminación.
- Copia do procedemento no que se estableza:
  - O período de retención dos rexistros de actividade e período de retención de evidencias tras un incidente.
  - Proceso para a eliminación dos rexistros tras o período estipulado de retención, incluíndo as copias de seguridade (se existen).
- Copia da política de copia de seguridade dos rexistros de actividade (se se segue unha política específica para este tipo de información, non incluída na política xeral de copia de seguridade de datos e sistemas (ver CBCS7)).
- Copia do procedemento para a centralización de logs, no que se indique as fontes orixe a centralizar, como se realizará a centralización, periodicidade, etc.
- Copia dunha revisión dos rexistros de auditoría realizada durante o ano e/ou dos resultados obtidos.

CBCS 7 Copia de seguridade de datos e sistemas

7.1.- Copia de seguridade de datos e sistemas

- Realízanse copias de respaldo que permitan recuperar datos perdidos cunha antigüidade determinada?

En canto á política de copia de seguridade :

- Inclúe datos (información de traballo) da entidade?
- Algún sistema, conxunto de datos, etc. queda fóra do alcance da política de copia?
- Abarca os datos de configuración, servizos, aplicacións, equipos, ou outros de natureza análoga?
- Se se utiliza criptografía para o cifrado da información, a política de copia inclúe o respaldo das claves criptográficas?
- Indicar tipo de copia e periodicidade (ex. Incremental diaria, completa semanal, etc.).
- Disponse de ferramenta/s para a realización de copias de seguridade? En caso afirmativo, indicar o nome da ferramenta, fabricante e versión.
- En que soporte se almacenan as copias de seguridade realizadas?
- Externalízanse as copias de seguridade? Onde? (ex. a un edificio distinto, a unha sala distinta dentro do mesmo edificio, ás instalacións dun provedor, etc.)
- Utilízanse servizos na nube para o almacenamento de backups? En caso afirmativo, indicar que servizo se utiliza e o provedor que o presta.

7.2.- Probas de recuperación

- Realízanse probas de recuperación a partir das copias de respaldo realizadas?
  - Indicar alcance das probas de recuperación e periodicidade.
  - Documéntanse (ou queda algún rexistro) da realización de ditas probas de recuperación e as incidencias identificadas?

7.3.- Protección dos backups

- Os backups gozan da mesma seguridade que os datos orixinais, tanto no seu acceso, almacenamento como transporte?

  Indicar brevemente os mecanismos utilizados para dito propósito.
- En canto a solicitudes puntuais de recuperación de datos por parte dos usuarios da organización, disponse dun procedemento que estableza como debe realizarse (quen pode solicitar, como, quen debe autorizar, etc.)?
- As copias de seguridade están accesibles de forma directa a nivel de rede?
- Disponse dunha copia de seguridade nun soporte desconectado da rede? Como e con que frecuencia se realiza?

Documentación necesaria:

- Copia do procedemento de copia de seguridade de datos e sistemas
- Copia do procedemento de restauración a partir das copias de seguridade realizadas
- Copia dos informes, rexistros, etc. das probas de recuperación realizadas no último ano
- Copia do procedemento para a solicitude de recuperacións puntuais de información a partir das copias de seguridade realizadas

CLCS 8 CUMPRIMENTO DE LEGALIDADE

8.1.- Esquema Nacional de Seguridade

- Dispón dunha política de seguridade escrita?
- Foi aprobada polo órgano superior competente (conforme ao Art. 11 do RD 3/2010)?
- Asignáronse os seguintes roles/responsabilidades? En caso afirmativo indicar nome e posto da persoa a quen se lle asignou.
  - Responsable/s da información
  - Responsable/s do servizo
  - Responsable da seguridade (STIC)
  - Responsable do sistema (TIC)
- Realizouse a auditoría de cumprimento do ENS para os sistemas de categoría Media e Alta? En caso afirmativo, indicar a empresa encargada da realización da auditoría.
- Para os sistemas de categoría Básica, realizouse a autoavaliación de cumprimento esixida no ENS ou ben, de forma opcional, a auditoría de cumprimento?
- Os resultados da auditoría e da autoavaliación foron revisados polo responsable de seguridade e as conclusións presentadas ao responsable do sistema para que adopte as medidas correctoras adecuadas?
- Facilita os datos necesarios para o Informe do Estado da Seguridade a través da ferramenta INES, cumprindo así a Instrución Técnica de Seguridade aprobada por resolución do 7 de outubro de 2016 ?

8.2.- LOPD/RGPD

- Designouse Delegado de Protección de Datos (DPD)? En caso afirmativo indicar nome e posto da persoa designada, indicando a súa posición no organigrama xeral da entidade.
- Comunicouse a súa designación á Axencia Española de Protección de Datos?
- Dispone de Rexistro de actividades de tratamento, de acordo ao establecido no artigo 30 do RGPD?
- Realizáronse as analises de risco dos tratamentos de datos persoais realizados pola entidade e as avaliacións de impacto para aqueles de risco alto?
- Como avalía e verifica a entidade a eficacia das medidas técnicas e organizativas (ex. mediante auditorías realizadas por empresas externas, autoavaliacións de cumprimento, etc.).

8.3.- Lei de Impulso da factura electrónica e creación do rexistro contable de facturas

- Dispone do informe de auditoría anual de sistemas esixido pola Lei 25/2013, do 27 de decembro de Impulso da factura electrónica e creación do rexistro contable de facturas?

Documentación necesaria:

- Copia da Política de seguridade requirida polo ENS
- Copia dos rexistros (ex. resolucións, actas, etc.) correspondentes á designación dos responsabes da información, do servizo, de seguridade e do sistema segundo o ENS
- Copia do informe de auditoría de cumprimento do ENS para os sistemas de categoría Media e Alta
- Copia da autoavaliación de cumprimento para os sistemas de categoría Básica segundo ENS
- Copia do documento que recolle os datos da última declaración na ferramenta INES
- Copia da designación do Delegado de Protección de Datos
- Copia do rexistro de actividades de tratamento de datos de carácter persoal

- Copia das analises de riscos e avaliacións de impacto dos tratamentos de datos persoais
- Nos casos nos que aplique, copia do informe de auditoría ou da autoavaliación da eficacia das medidas de seguridade aplicadas aos datos persoais
- Copia do informe de auditoría de sistemas esixido no Art. 12.3. da Lei 25/2013, do 27 de decembro de Impulso da factura electrónica e creación do rexistro contable de facturas