INSTRUCIÓNS:

O seguinte cuestionario pretende ampliar o coñecemento dos sistemas de información da entidade, enmarcado dentro das actividades de planificación da auditoría realizada pola Sindicatura / Cámara de Contas.

A información obtida a través do presente cuestionario servirá de base para futuros traballos, nos que só será necesaria a súa actualización.

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 da 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.).

A1 - CBCS 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?
- Dispónse de Rexistro de actividades de tratamento, de acordo ao establecido no artigo 30 do RGPD?
- Realizáronse os analisis 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)

- Dispónse 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?

8.4.- Cumprimento do Esquema Nacional de Interoperabilidade.

- Atópanse os sistemas adecuados aos criterios e recomendacións establecidos no Esquema Nacional de Interoperabilidade (Disposición transitoria RD 4/2010)?
- Na súa falta, existe o Plan de Adecuación ao Esquema Nacional de Interoperabilidade e atópase formalmente aprobado?

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
- Copia do Plan de Adaptación ao Esquema Nacional de Interoperabilidade

A.2: ESTRATEXIA DE SEGURIDADE

A.2.1: Planificación estratéxica dos SI

- Existe un Plan Estratéxico dos Sistemas de TI?

A.2.1: Planificación Anual de Proxectos de SI

- Existe un Plan Anual de Proxectos de SI?

A.2.1: Dotación Orzamentaria para Proxectos de SI

- Existe dotación orzamentaria para os proxectos incluídos no Plan Anual de Proxectos de SI?

Documentación necesaria:

- Copia do Plan Estratéxico de Sistemas de Información
- Copia do Plan Anual de Proxectos e Investimento en TI
- Evidencia das partidas orzamentarias dedicadas aos investimentos de TI

A.3: ORGANIZACIÓN E PERSOAL DE TI

A.3.1: Independencia Funcional

- É o departamento de sistemas de información independente doutras áreas funcionais?
- Depende o departamento de sistemas de información directamente da dirección?

A.3.2: Segregación de Funcións

- Existe segregación de funcións e tarefas?
- En caso afirmativo, sepáranse como mínimo as seguintes funcións?
  - Operacións
  - Administración (configuración, mantemento)
  - Supervisión (auditoría, goberno)

A.3.3: Formación e Concienciación

- Realízanse accións para concienciar regularmente ao persoal acerca do seu papel e responsabilidade sobre a seguridade dos sistemas e a información contida neles?
- Forma parte do contido das accións de concienciación a normativa de seguridade relativa ao bo uso dos sistemas?
- Fórmase regularmente ao persoal naquelas materias relativas á seguridade da información e dos sistemas que lle sexan de aplicación para o desempeño das súas funcións?

A.3.4: Indicadores de Cumprimento de Obxectivos

- Utilízanse indicadores por parte da dirección para valorar o cumprimento de obxectivos estratéxicos de TI?

A.3.5: Nomeamentos e Constitución de Órganos

- Realizáronse os nomeamentos requiridos para asegurar o cumprimento normativo e organización da seguridade?
- Constituíronse os órganos de goberno necesarios para asegurar o cumprimento normativo e organización da seguridade?

Documentación necesaria:

- Organigrama xeral da entidade (incluíndo a área de tecnoloxía).
- Organigrama da área de tecnoloxía.
- Documento de funcións e responsabilidades de cada unha das subáreas de tecnoloxía.
- Copia do Plan de Formación.
- Copia do Plan de Concienciación.
- Documentación acreditativa do uso de indicadores de cumprimento nos obxectivos estratéxicos de TI por parte da dirección.
- Copia das Actas de Nomeamento dos roles de seguridade.
- Copia das Actas de Constitución dos Órganos de Goberno de Seguridade

A.4: MARCO NORMATIVO E PROCEDEMENTAL DE SEGURIDADE

A.4.1: Normativa Interna de Seguridade

- Dispón dun ou varios documentos que constitúan a Normativa de Seguridade da Entidade?
- Dita normativa, especifica cal é o uso correcto de equipos, servizos, instalacións e sistemas?
- Especifica dita normativa a responsabilidade do persoal con respecto ao cumprimento ou violación destas normas, incluíndo dereitos, deberes e medidas disciplinarias?

A.4.2: Procedementos de Seguridade

- Dispón dun ou varios documentos que constitúan os procedementos de seguridade escritos?
- Precisan os procedementos como levar a cabo as tarefas habituais?
- Precisan os procedementos quen debe realizar cada tarefa?

Documentación necesaria:

- Copia da Normativa Interna de Seguridade.
- Copia dos Procedementos de Seguridade aprobados.

B.1: ADQUISICIÓN DE APLICACIÓNS E SISTEMAS

B.1.1: Procedemento de Adquisición de Aplicacións e Sistemas

- Existe un procedemento formal para planificar e executar a adquisición de novas aplicacións, sistemas ou compoñentes de sistemas?
- O Procedemento de Adquisición de Aplicacións e Sistemas ten en consideración os obxectivos de seguridade definidos pola entidade? De que forma se articula dita consideración?

B.1.2: Adquisición de Aplicacións e Sistemas por Obxectivos Estratéxicos e de Seguridade

- O Procedemento de Adquisición de Aplicacións e Sistemas ten en consideración os obxectivos estratéxicos e de negocio da entidade? De que forma se articula dita consideración?

B.1.3: Dimensionamento na Adquisición de Aplicacións e Sistemas

- O Procedemento de Adquisición de Aplicacións e Sistemas inclúe o dimensionamento adecuado considerando as necesidades actuais e futuras?
- En caso afirmativa, considérase para o dimensionamento as necesidades relativas o seguinte?
  - necesidades de procesamento
  - necesidades de almacenamento
  - necesidades de comunicación
  - necesidades de persoal
  - de instalacións e medios auxiliares

B.1.4: Adquisición de Aplicacións e Sistemas Avaliadas desde o punto de vista da Seguridade

- De acordo ao Procedemento de Adquisición de Aplicacións e Sistemas utilízanse ou adquírense, produtos ou equipos cuxas funcionalidades de seguridade e o seu nivel fosen avaliados conforme a normas europeas ou internacionais?

Documentación necesaria:

- Copia do procedemento Adquisisión de Aplicacións e Sistemas
- Copia de estudos previos á adquisición de aplicacións ou sistemas adquiridos

B.2: DESENVOLVEMENTO DE APLICACIÓNS

Identifique as aplicacións que soportan os principais procesos de negocio.

Clasifique cada unha das aplicacións identificadas segundo a seguinte taxonomía:

- Software propio desenvolvido pola organización.
- Software comprado con pequenas ou ningunha personalización.
- Software comprado con personalización significativa.
- Software propiedade dunha empresa de Outsourcing.

B.2.1: Metodoloxía de Desenvolvemento

- Utilízase unha metodoloxía de desenvolvemento recoñecida para o desenvolvemento de aplicacións e sistemas? Cal é a metodoloxía utilizada?
- En caso afirmativo, considera dita metodoloxía a seguridade de forma integral ao longo do ciclo de desenvolvemento?
- En caso contrario, realiza durante o ciclo de vida do desenvolvemento as seguinte actividades?:
    - Análise de requisitos
    - Análise de viabilidade
    - Deseño seguro
    - Construción e probas
    - Deseño da posta en explotación e aceptación

B.2.2: Contornas de Desenvolvemento

- Desenvólvense as aplicacións ou sistemas sobre unha contorna diferente e separada do de produción?

B.2.3: Aceptación e posta en servizo

- Dispón dun plan de probas antes de pasar a produción para comprobar o correcto funcionamento da aplicación?
- En caso afirmativo, inclúe dito plan probas de seguridade como criterios de aceptación?
- Requírese da aprobación do usuario nas probas de testeo previamente ao paso a produción?
- Realízanse as probas nunha contorna illada ou na contorna de produción?

Documentación necesaria:

- Copia do procedemento ou metodoloxía utilizada para o desenvolvemento de sistemas e aplicacións.
- Exemplo de documentación xerada no ciclo de vida de desenvolvemento dun sistema.

B.3: XESTIÓN DE CAMBIOS

B.3.1: Procedementos para a xestión de cambios de configuración do sistema

- Xestiónase de forma continua a configuración de aplicacións e sistemas?
- En caso afirmativo existe un procedemento para iso?
- Utilízase algunha ferramenta para automatizar a xestión de cambios na configuración dos sistemas?
- Contempla o procedemento ou a práctica común dos cambios de configuración os seguintes puntos?:
    - Rexistro de solicitudes
    - Avaliación
    - Autorización
    - Probas
    - Planificación de posta en operación
    - Rexistro de cambios
- A avaliación do cambio inclúe a análise do risco desde o punto de vista da seguridade?

B.3.2: Procedementos para a xestión de cambios de compoñentes ou arquitectura do sistema

- Xestiónanse de forma continua os cambios de compoñentes e/ou arquitectura de aplicacións e sistemas?
- En caso afirmativo existe un procedemento para iso?
- Contempla o procedemento ou a práctica común dos cambios de compoñentes e/ou arquitectura os seguintes puntos?:
    - Rexistro de solicitudes
    - Avaliación
    - Autorización
    - Probas
    - Planificación de posta en operación
    - Rexistro de cambios
- ¿ avaliación do cambio inclúe a análise do risco desde o punto de vista da seguridade?

B.3.3: Responsables e órganos para a xestión de cambios de aplicacións ou sistemas

- Asignáronse responsabilidades para a xestión continuada de cambios en aplicacións e sistemas?
- Constituíronse organos para a xestión continuada de cambios en aplicacións e sistemas?

B.3.4: Probas de testeo dos cambios en aplicacións e sistemas

- Realízanse probas de testeo dos cambios antes da posta en operación?
- Que tipo de probas se realizan?

B.3.5: Contornas para probas separadas de produción

- Realízanse probas de testeo dos cambios en contornas separadas da produción?

B.3.6: Aprobación do usuario nas probas de testeo

- Requírese da aprobación do usuario para a aceptación das probas de testeo previas á posta en operación?

B.3.7: Separación das tarefas para a xestión de cambios de aplicacións ou sistemas

- A execución das distintas accións e responsabilidade no proceso de xestión de cambios, é realizada por distintas persoas?
- Realízase o control dos accesos ás distintas contornas utilizado para desenvolvemento e probas de testeo en aplicacións e sistemas de acordo á separación de funcións implantada no proceso de xestión de cambios?

B.3.8: Rexistro de cambios e solicitudes

- Realízase a xestión documental e o rexistro das peticións e os cambios nas aplicacións e sistemas significativos?

Documentación necesaria:

- Copia do procedemento de Xestión de Cambios
- Copia do procedemento de procedemento de Xestión da Configuración
- Copia das actas de constitución dos organos de xestión de cambios
- Exemplo de resultado de proceso completo de tramitación dun cambio de configuración dun sistema.
- Exemplo de resultado de proceso completo de tramitación dun cambio de arquitectura ou compoñente dun sistema.

C1 - 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 se 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.

C1 - 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 (ex.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.

C2 - 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 análises 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.

C3 - 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 plantillas 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?

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 "monitorizar" en tempo real a configuración de seguridade de todos 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 monitoricen 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.

C4 - 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 sexa 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?
- Dispone 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

- Dispone 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.

C.5: SERVIZOS EXTERNOS

C.5.1.- Nivel de Cumprimento do Servizo

- Dispón a entidade dun procedemento de Contratación de Servizos Externos que documente os pasos previos á contratación de servizos incluíndo o detalle por parte do provedor das características do servizo para prestar e os requisitos de servizo e seguridade requiridos?
- Inclúese nos contratos asinados co provedor ditos acordos de nivel de servizo estipulados no procedemento de contratación?
- Detállase no contrato as responsabilidades de ambas partes?
- Inclúese no contrato as consecuencias do incumprimento dos acordos?

C.5.2.- Xestión do Nivel de Cumprimento do Servizo

- Disponse dun sistema rutineiro para medir o cumprimento das obrigas de servizo?
- Establecéronse mecanismos para a xestión das desviacións en indicadores incluídos nos acordos de nivel de servizo?
- Establecéronse mecanismos para a xestión de incidentes durante o desempeño do servizo?

C.5.3.- Requisitos de Seguridade dos Servizos Externos

- Transmitiuse ao provedor de servizo as súas obrigas sobre a seguridade dos sistemas que provén servizo á administración mediante a inclusión de clausulas nos contratos?
- Inclúen ditas clausulas as medidas de seguridade necesarias para o cumprimento do ENS e son as incluídas na Declaración de Aplicabilidade?

C.5.4.- Xestión da Seguridade dos Servizos de Cloud

- Transmitiuse ao provedor de servizo as obrigas adicionais sobre a seguridade dos sistemas que provén servizos de Cloud á administración mediante a inclusión de clausulas nos contratos?
- Incluíronse entre ditas obrigas particulares as seguintes?:
    - Se os elementos de seguridade como Firewalls son virtualizados, non deben residir nas mesmas máquinas que os compoñentes de produción.
    - O hypervisor atópase particularmente protexido mediante medidas adicionais ao seu nivel, particularmente en conto a identificación, autenticación e autorización de administradores.
    - A rede de xestión dedicada ao servizo é distinta a outras redes das que dispoña o provedor, incluíndo os equipos de conexión a internet para acceso remoto.
    - Non se comparten equipos hypervisor para sistemas de distinta clasificación.
    - A administración do hypervisor está diferenciada da administración dos elementos virtualizados.

Documentación necesaria:

- Copia do procedemento de Contratación de Servizos Externos
- Exemplo de contrado de servizos externos.

C.6 PROTECCIÓN FRONTE A MALWARE

C.6.1.- Protección Fronte a Código Daniño

- Dispón de mecanismos de prevención e reacción fronte a código daniño (virus, vermes, troianos, programas espía e "malware" en xeral)?
- Segue as directrices de configuración, mantemento e actualización do fabricante?
- Que mecanismos de actualización utiliza? Con que periodicidade? Actualiza BBDD de Sinaturas? Actualiza os postos cliente?
- Que funcionalidades do produto ten instaladas?
- Como protexe a aquilo equipos que non poden instalar o software de protección corporativo?

C.6.2.- Protección de Correo electrónico

- Protéxese á organización fronte a problemas que se materializan por medio do correo electrónico como correo non desexado (spam)? Que mecanismos se utilizan?
- Dispón a organización de ferramentas para protexerse fronte a código daniño no Correo electrónico?
- Estableceuse normativa de uso do Correo electrónico e comunicouse aos usuarios?

Documentación necesaria:

- Copia do procedemento de seguridade fronte a código daniño ou normativa específica

C.7 PROTECCIÓN DE INSTALACIÓNS E INFRAESTRUTURA

C.7.1.- Control de Accesos a Instalacións

- Disponse de distintas localizacións para o equipamento segundo a súa función?
- Contrólanse os accesos a ditos locais de acordo a unha política de identificación e autorización? Que métodos se utilizan?
- Que criterios se utilizan para proporcionar dereitos de acceso?
- Rexístranse os accesos?

C.7.2.- Infraestrutura en CPD

- Dispón o CPD e os centros de cableado da infraestrutura física necesaria para o cableado e a instalación dos sistemas?
- Disponse de canalizacións independentes para enerxía e datos? Respéctanse as distancias mínimas?
- Disponse de falso chan e/ou teito no CPD e os centros de cableado principais?

C.7.3.- Acondicionamento de Locais

- Os locais onde se sitúan os sistemas de información e os seus compoñentes dispoñen de sistemas para adecuar as condicións de temperatura e humidade?
- Atópanse ditos sistemas dimensionados de acordo ao consumo electrico e produción de calor actuais?
- Configurouse o CPD considerando a óptima disipación da calor, por exemplo mediante a impulsion de aire por chan técnico e o uso de corredores fríos e quentes?

C.7.4.- Subministración Eléctrica

- Garántese a subministración de potencia eléctrica? Realizouse unha análise da potencia eléctrica necesaria?
- Garántese a alimentación ininterrompida ante fallo da subministración eléctrica mediante o uso de SAIS?
- Dimensionáronse os SAIS para proporcionar aos sistemas críticos o tempo suficiente para un apagado seguro?
- Proporciónase a subministración eléctrica mediante acometidas redundantes? Proveñen de distintos cadros eléctricos? Proveñen de distintos centros de transformación? (Control E3)
- Existen métodos alternativos de subministración de enerxía en caso de fallo prolongado do servizo do provedor? Disponse de grupo electróxeno fixo ou móbil?

C.7.5.- Protección Fronte a Incendios

- Disponse en CPDs e locais onde se sitúan os sistemas de información de sistemas e medidas de protección fronte a incendios? Cales son?
- Cumpren ditos sistemas coa normativa industrial existente?
- Atópanse ditos sistemas comunicados a centrais de alarmas?
- Considerouse a protección pasiva contra incendios para o deseño dos elementos de CPD, tales como cubertas de cableados, portas ou materiais de falso teito e chan?

C.7.6.- Protección Fronte a Inundacións

- Protéxense os locais onde se sitúen os sistemas de información e os seus compoñentes fronte a incidentes fortuítos ou deliberados causados pola auga?
- Utilízanse sensores para a detección de humidade e auga no CPD?
- Realizouse o deseño do CPD e dos locais onde se sitúan os sistemas de información de acordo a criterios para evitar o risco por causado pola auga?

Documentación necesaria:

- Documentación técnica de infraestruturas e elementos construtivos do CPD.
- Procedemento de control de acceso físico aos locais onde se sitúen os sistemas de información.

C.8 XESTIÓN DE INCIDENTES

C.8.1.- Detección de Incidentes e Eventos dos Sistemas

- Disponse de ferramentas que permitan a xestión e detección temperá de incidentes de seguridade nos sistemas?
- Disponse de persoal asignado ao tratamento dos eventos detectados?

C.8.2.- Xestión de Incidentes

- Dispón dun proceso integral para facer fronte a incidentes que poidan ter un impacto na seguridade do sistema?
- Atópase dito proceso plasmado nun procedemento?
- Inclúe dito procedemento o escalado ao responsable para a xestión do incidente?

C.8.3.- Resposta ante Incidentes

- Inclúe a toma de medidas urxentes para a resolución do incidente?
- Inclúe a asignación de recursos para investigar as causas, analizar as consecuencias e resolver o incidente?

C.8.4.- Comunicación de Incidentes

- Inclúe o procedemento o proceso de notificación por parte do usuario ou administrador do sistema que detecte o incidente?
- Inclúe o procedemento a notificación ao responsable para a xestión do incidente?
- Inclúe o procedemento a notificación ás partes interesadas?

C.8.5.- Prevención de Incidentes e Mellora Continua

- Inclúe o procedemento accións para evitar a repetición de incidentes detectados?
- Inclúe o procedemento un proceso de mellora continua para a optimización na xestión de incidentes?

Documentación necesaria:

- Copia do procedemento de Xestión de Incidentes

C.9 Monitorización

C.9.1.- Ferramenta de monitorización de redes e sistemas

- Disponse de ferramentas que permitan a monitorización do estado de redes e sistemas?
- Disponse de persoal asignado á monitorización do estado dos sistemas?

C.9.2.- Linea Base dos Sistemas

- Proporciona a ferramenta de monitorización información adecuada para establecer unha liña base de utilización que pode ser explotada por equipo de TI?
- Utilízase a ferramenta de monitorización para a detección de incidentes en base a comportamentos anómalos?
- Utilízase a ferramenta de monitorización para a planificación estratéxica e o dimensionamento de novos sistemas de información?

C.9.3.- Rexistro de Eventos

- Proporciona a ferramenta información sobre os eventos detectados nas redes e sistemas?
- Permite a ferramenta a correlación de eventos para identificar causa raiz de incidentes?
- Permite a ferramenta a consulta de datos historicos para análise forense de incidentes de seguridade?

Documentación necesaria:

- ¿?

D1 - 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/renoméanse 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
Ex: SGBD Oracle 11.2	Contrasinal	….
Ex: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.

D.2 MECANISMOS DE IDENTIFICACIÓN E AUTENTICACIÓN

D.2.1.- Procedemento de Identificación e Autenticación de Usuarios

- Disponse dun procedemento de xestión que contemple os mecanismos utilizados para a identificación e autenticación dos usuarios?

D.2.2.- Identificación de Usuarios

- Disponse de identificadores singulares de usuario para o acceso aos sistemas?
- Cada usuario que accede ao sistema ten asignado distintos identificadores únicos en función de cada un dos roles que deba desempeñar no sistema?
- Inhabilítase o identificador cando o usuario deixa a organización, cesa na función para a cal se requiría a conta de usuario ou cando a persoa que a autorizou dá orde en sentido contrario?
- Se o identificador debe ser eliminado, mantense durante o período necesario para atender ás necesidades de trazabilidade dos rexistros de actividade asociados ás mesmas?

D.2.3.- Auntenticación de Usuarios

- Cal é o mecanismo de autenticación dos sistemas segundo o seu nivel?
- O algoritmo de autenticación está acreditado ou certificado?
- Implantouse unha política de contrasinais que fixe a calidade mínima e o período para a renovación da mesma?
- Utilízase dobre factor de autenticación nalgún caso?
- Retíranse e deshabilitanse as credenciais cando o usuario que autentican termina a súa relación co sistema?
- Suspéndense as credenciais tras un período definido de non utilización?

Documentación necesaria:

- Procedemento de Xestión de Usuarios /Identificación /Autenticación /Xestión de Contrasinais/ Xestión de Dereitos de Acceso

D.3 XESTIÓN DE DEREITOS DE ACCESO

D.3.1.- Procedemento de Xestión de Dereitos de Acceso

- Disponse dun procedemento de xestión que contemple a mecanismos utilizados para o control dos dereitos de acceso dos usuarios aos sistemas?

D.3.2.- Mecanismos de Control dos Accesos

- Contan os sistemas críticos con mecanismos de control de accesos que impidan a utilización dos seus recursos?
- Establécense os dereitos de acceso de cada recurso segundo as decisións da persoa responsable do recurso, aténdose á política e normativa de seguridade do sistema?
- Os mecanismos de control de accesos, inclúen a distinción no acceso aos distintos recursos do sistema e aos ficheiros de configuración?
- Rexístranse os accesos con éxito e os errados?
- Limítase o número de intentos errados de acceso?
- Informa o sistema ao usuario das súas obrigas para obter o acceso?
- Limítase o horario, datas e lugar desde onde se accede?
- Establecéronse puntos nos que o sistema requirirá unha renovación da autenticación do usuario?

D.3.3.- Principio para a Asignación de Dereitos de Acceso

- Limítanse os privilexios de cada usuario ao mínimo estritamente necesario para acceder á información requirida e para cumprir as súas obrigas?
- Pode só e exclusivamente o persoal con competencia para iso conceder, alterar ou anular a autorización de acceso aos recursos conforme aos criterios establecidos polo seu responsable?

Documentación necesaria:

- Procedemento de Xestión de Usuarios /Identificación /Autenticación /Xestión de Contrasinais/ Xestión de Dereitos de Acceso

D.4 XESTIÓN DE USUARIOS

D.4.1.- Procedemento de Xestión de Usuarios

- Disponse dun procedemento de xestión dos usuarios dos sistemas?

D.4.2.- Definición de Postos de Traballo

- Caracterizouse cada posto de traballo?
- Inclúe dita caracterización a definición das responsabilidades relacionadas co posto de traballo?
- Inclúe dita caracterización a definición dos dereitos de acceso sobre os sistemas?

D.4.3.- Xestión Continuada dos Dereitos dos Usuarios

- Realiza a entidade a xestión dos usuarios do sistema e os seus privilexios de acordo ás súas obrigas e responsabilidades?
- Revisa periodicamente a actividade dos usuarios para identificar os usuarios inactivos?
- Revisa periodicamente as baixas na entidade e as diferenzas cos usuarios activos?

Documentación necesaria:

- Procedemento de Xestión de Usuarios /Identificación /Autenticación /Xestión de Contrasinais/ Xestión de Dereitos de Acceso

D.5 PROTECCIÓN DE REDES e COMUNICACIÓNS

D.5.1.- Protección por Firewall

- Dispón de dispositivo Firewall que realice funcións de control de acceso exterior?
- Dispón o Firewall dalgunha das seguintes funcionalidades avanzadas?:
    - IDS
    - IPS
    - DPI (Deep Packet Inspection)
    - Application Inspection
    - DLP (Data Leak Prevention)
    - Inspección de tráfico encriptado
- Mantense adecuadamente actualizado o firewall en canto a firmas e outra información de terceiros para o procesado de seguridade?

D.5.2.- Arquitectura de Rede

- Realizouse un deseño considerando o uso de DMZ para aloxar aos elementos que requiren comunicación co exterior?
- En caso de existir DMZ, son os firewalls internos e externos de distintos fabricantes?
- Dispoñen os sistemas de Firewall da adecuada redundancia hardware?

D.5.3.- Conexións Exteriores Seguras

- Empréganse redes privadas virtuais (VPN) cando a comunicación discorre por redes fora do propio dominio de seguridade?
- Utilizan ditas conexións privadas vistuales algoritmos acreditados polo CCN?

D.5.4.- Segmentación de Redes

- Atópase a rede segmentada?
- Que criterio se utiliza para o deseño e dimensionamiento da segmentación?
- Cal é o tamaño máximo por segmento?
- Atópase o dispositivo de interconexión (Firewall, Router) entre segmentos particularmente monitorizado e protexido?

D.5.5.- Mecanismos de Identificación e Autenticación para Xestión de Rede

- Utilízanse configuracións seguras para a identificación e autenticación de administradores dos sistemas de comunicacións e electrónica de rede?
- Utilízanse conexións seguras como SSH? deshabilitouse o acceso por telnet?
- Implementáronse mecanismos de encriptación de contrasinais na configuración dos equipos de comunicacións?
- Implementáronse mecanismos de autenticación baseados no uso de servidores de autenticación, utilizando protocolos de autenticación como RADIUS ou TACACS?

D.5.6.- Xestión segura de Logs e Notificacións

- Impleméntanse configuracións seguras para xestionar os eventos e notificacións dos sistemas de comunicacións?
- Utilízanse repositorios externos para a recepción e tratamiento das notificacións xeradas polos equipos de comunicacións e electrónica de rede?
- Utilízanse protocolos seguros para a comunicación de eventos e notificacións? Utilízase SNMPv3 e deshabilitouse o uso de protocolos obsoletos como SNMPv1 ou SNMPv2?

D.5.7.- Configuracións por Defecto e Automáticas

- Utilízase no equipamento de comunicacións e electrónica de rede configuracións automáticas?
- Utilízase configuración dinámica de trunks?
- Utilízase configuración dinámica de vlans?
- Utilízase configuración dinámica de Etherchannels?
- Utilízanse no equipamento de comunicacións e electrónica de rede configuracións por defecto?
- Atópase a vlan 1 utilizada na electrónica de rede?
- Mantéñense habilitados por defecto os portos da electrónica de rede?
- Deshabilitouse o servidor web embebido nos dispositivos de electrónica de rede?
- Atópase deshabilitada a conexión á electrónica de rede mediante protocolo telnet?
- Atópase deshabilitado o servidor FTP embebido na electrónica de rede?
- Modificáronse a comunity string por defecto de SNMPv1 e v2?
- Deshabilitouse o uso de versións anteriores a SNMPv3?
- Modificouse o prompt por defecto?

D.5.8.- Mecanismos contra Ataques LAN

- Utilízanse mecanismos de seguridade para evitar ataques na rede de área local? Cales son ditos mecanismos?

D.5.9.- Control de Acceso aos Recursos de Rede

- Utilízanse mecanismos para limitar o acceso a recursos da rede? Cales son ditos mecanismos?
- Utilízase 802.1x para o control perimetral?
- Protéxense as comunicacións para a xestión de routing dinámico (se se emprega) mediante mecanismos de acutenticación?
- Protéxense as comunicacións dos protocolos de alta dispoñibilidade?

Documentación necesaria:

- ¿?

E1 - 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

E.2 PLAN DE CONTINUIDADE

E.2.1.- Identificación de Elementos Críticos da Actividade

- Realizouse unha Análise de Impacto na Actividade para identificar os servizos críticos?
- Identificáronse os requisitos de dispoñibilidade dos servizos?
- Identificáronse os sistemas e elementos que sosteñan os servizos críticos?

E.2.2.- Plan de Continuidade da Actividade

- Dispón dun Plan de Continuidade da Actividade?
- Identifica os roles, as súas responsabilidades e as funcións para realizaren caso de crise?
- Existe unha previsión de medios alternativos para permitir a continuidade do servizo?
- Recibiu o persoal involucrado no PCN a formación necesaria para exercitar as súas funcións?
- É parte doutros plans da entidade que transcenden dos Sistemas de Información e a súa seguridade?

E.2.3.- Probas do Plan de Continuidade da Actividade

- Realízanse probas periódicas para localizar e corrixir, no seu caso, os erros ou deficiencias que poidan existir no plan de continuidade?
- Con que periodicidade se realizan?
- Lévase a cabo a totalidade das accións do Plan ou limítase o alcance en cada proba?

Documentación necesaria:

- Plan de Continuidade da Actividade / Plan de Recuperación de Desastres
- Análise de Impacto na Actividade

E.3 ALTA DISPOÑIBILIDADE

E.2.1.- Deseño enfocado á Alta Dispoñibilidade

- Considérase a Alta Dispoñibilidade como criterio no deseño, adquisición e desenvolvemento dos sistemas?

E.2.2.- Localizacións Redundantes

- Disponse de localizacións redundantes para os locais de que albergan sistemas de información ou elementos crítiticos dos mesmos?
- Dispón de CPD redundado?
- Atópanse redundados os centros de cableado principais?

E.2.3.- Elementos Redundantes de Sistemas Críticos

- Dispón de redundancia eléctrica nos locais que albergan sistemas de información?
- Atópanse redundados e discorren por camiños e canalizacións independentes as ligazóns de comunicacións que proporcionan servizo a elementos críticos da rede?
- Atópanse redundados os equipos de comunicacións que realizan tarefas críticas na rede?.
- Dispoñen de dobre fonte de alimentación os equipos de comunicacións que realizan tarefas críticas na rede?
- Dispoñen de dobre tarxeta supervisora os equipos de comunicacións que realizan tarefas críticas na rede?
- Encóntranse redundados en localizacións distintas os servidores que realizan tarefas críticas ou albergan a execución de aplicacións críticas?
- Dispoñen de dobre fonte de alimentación os servidores que realizan tarefas críticas ou albergan a execución de aplicacións críticas?

Documentación necesaria:

- Copia do procedemento ou metodoloxía utilizada para o desenvolvemento de sistemas e aplicacións.
- Copia do documento de arquitectura básica dos sistemas