Adecuación al Esquema Nacional de Seguridad del Ayuntamiento de CiudadX

Según la versión 2022 del Esquema Nacional de Seguridad

Adrián Capdevila Dueñas
Grado de Ingeniería Informática
Área de Seguridad Informática

Nombre Tutor/a de TF
Jorge Miguel Moneo

Profesor/a responsable de la asignatura
Andreu Pere Isern Deyà

Universitat Oberta
de Catalunya

Fecha Entrega 13 de junio de 2023

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Adecuación al Esquema Nacional de Seguridad del Ayuntamiento de CiudadX*
Nombre del autor:	*Adrián Capdevila Dueñas*
Nombre del consultor/a:	*Jorge Miguel Moneo*
Nombre del PRA:	*Andreu Pere Isern Deyà*
Fecha de entrega:	*13/06/2023*
Titulación o programa:	Grado de Ingeniería Informática
Área del Trabajo Final:	*Seguridad Informática*
Idioma del trabajo:	*Castellano*
Palabras clave	*Esquema Nacional de Seguridad, Análisis de riesgos, Ciberseguridad normativa*

Resumen del Trabajo

El proyecto documenta la adecuación al Esquema Nacional de Seguridad de un ayuntamiento ficticio (CiudadX), concretamente a la versión publicada en 2022 que ha supuesto la primera gran actualización de este desde su lanzamiento en 2010, tanto en controles de seguridad como en la estructura general, incluyendo los requisitos y principios básicos.

El reciente impulso que ha recibido el esquema para aumentar su grado de implantación, sumados al alarmante número de entidades locales que están sufriendo ataques de ransomware, han hecho que CiudadX decida dar sus primeros pasos para securizar sus sistemas, y decide hacerlo bajo el marco de ENS, para, a medio plazo, certificar su conformidad.

CiudadX tiene una población cercana a los 25.000 habitantes, por lo que, dado su tamaño, cuenta con variedad de servicios TIC necesarios para el gobierno de su información y el buen funcionamiento de la localidad.

Este trabajo contempla el ciclo completo de implantación del Esquema Nacional de Seguridad siguiendo las guías oficiales del CCN-CERT, desde la definición de una política de seguridad, la identificación y valoración de sistemas, hasta las fases finales de seguimiento de métricas y mejora continua, así como la ejecución de tareas de adecuación a modo de ejemplo.

Abstract

The project documents the adequation to the Esquema Nacional de Seguridad of a fictitious town hall (CiudadX), concretely to the version published in 2022, which has meant the first major update of the law since its launch in 2010, specially in security controls and in its general structure, including the requirements and basic principles.

The recent boost that the law has received to enhance its implementation, plus the increasing number of town halls that are suffering ransomware attacks, have convinced CiudadX to take its first steps to secure its systems. It will be done by the ENS framework, to, in the medium term, certify its compliance.

CiudadX has a population of close to 25,000 inhabitants, therefore, given its size, it has a variety of ICT services necessary for the government of its information and the proper functioning of the town.

This work covers the complete implementation cycle of the ENS following the official guidelines of the CCN-CERT, since the definition of a security policy, the identification and assessment of systems, up to the final phases of monitorization metrics and continuous improvement, as well as the execution of some compliance tasks as an example.

Índice

Lista de ilustraciones

Lista de tablas

1 Introducción

1.1. Contexto y justificación del Trabajo

En 2007 se publicó la ley 11/2007 que regulaba el acceso electrónico de los ciudadanos a los Servicios Públicos, la cual garantizaba su derecho a acceder telemáticamente a los trámites administrativos.

En el marco de dicha ley, 3 años más tarde, se publicó la **primera versión del Esquema Nacional de Seguridad** (en adelante ENS) con el objetivo claro de crear un entorno de confianza y ciberseguridad en dichos trámites.

Aquella versión del ENS, al estar centrada en la tramitación online, ponía el foco en la securización de las sedes electrónicas y los componentes accesorios que les daban servicio, asentando las bases de la diligencia con la que las administraciones públicas debían tratar los datos informatizados de los ciudadanos.

A la publicación del ENS le han acompañado numerosas **guías de seguridad** publicadas por el Centro Criptológico Nacional, que desarrollan algunos apartados del ENS o incluyen recomendaciones para su implantación. A toda esta serie de documentos se les ha asignado la nomenclatura “serie 800”, siendo hoy en día la serie que más actualizaciones y nuevos documentos recibe cada año.

Además de dichas guías, para facilitar la adecuación a determinados colectivos, se han publicado “perfiles de cumplimiento”, que son listados particularizados de medidas de seguridad que sustituyen o simplifican los controles del ENS para tipos concretos de organización. Para los ayuntamientos se han publicado 3 de estos perfiles, adecuando cada uno a los diferentes tamaños, de los cuales es el tercero (el más restrictivo), el que afectaría a CiudadX:

- Perf. de Cumplimiento Ayuntamientos <5.000 habitantes
- Perf. de Cumplimiento Ayuntamientos <20.000 habitantes
- Perf. de Cumplimiento Ayuntamientos 20.000> <75.000 habitantes

A pesar de que el ENS fue de obligado cumplimiento desde su nacimiento, a los sistemas antiguos se les concedió un periodo de adecuación de 4 años (hasta 2014), pero hoy en día, 13 años después, según el CCN-CERT[1], **sólo 28 de los 8000 ayuntamientos de España, han conseguido la certificación del ENS**.

[1]Centro Criptológico Nacional (CCN) (2023) Disponible en: https://gobernanza.ccn-cert.cni.es/certificados (Consultada el 1 de abril de 2023)

Cabría esperar que, aunque el cumplimiento normativo no haya sido notorio, el nivel de protección de los ayuntamientos fuera satisfactorio, pero la cantidad de ayuntamientos que están siendo víctimas de ataques exitosos de ransomware[2][3][4], pone de manifiesto que es necesario acelerar la implantación de mejoras.

Posteriormente, en 2022 se ha producido la primera **gran revisión y actualización del ENS**, la cual ha introducido numerosas modificaciones que hacen que todos los sistemas deban ser reevaluados, se deban replantear los controles aplicados, y que amplía el alcance a muchos otros sistemas incluyendo a proveedores.

Esta nueva versión supone una **oportunidad** para que aquellas organizaciones que no han completado su adecuación lo hagan directamente con una versión más moderna, que afronta riesgos y amenazas actuales, y que dispone de herramientas más flexibles (como los perfiles de cumplimiento o los controles de refuerzo) que la versión inicial.

Las principales **herramientas** de que disponen las organizaciones para conseguir esta adecuación (las mismas que se van a utilizar para realizar este proyecto), son el propio **texto del ENS**, las **guías de la serie 800 mencionadas la bibliografía** del presente documento, así como la metodología de análisis de riesgos **MAGERIT v3**.

En cuanto a **competidores**, existen multitud de empresas que ayudan a los organismos y proveedores a cumplir con el ENS, aunque siendo que persiguen fines comerciales y no divulgativos, no deben considerarse competencia directa. En todo caso, el presente trabajo vendría a complementar las propias guías del CCN-CERT por la labor divulgativa que realizan.

1.2. Objetivos del Trabajo

Teniendo en cuenta la cantidad de novedades de la nueva versión y la falta de ejemplos actualizados disponibles públicamente, se ha decidido documentar la implantación del nuevo ENS en el ayuntamiento de la ciudad ficticia CiudadX con los siguientes objetivos:

1. **Analizar y destacar aquellos apartados que sean significativamente diferentes de la versión inicial del ENS**, de modo que pueda servir de guía para aquellas organizaciones que iniciaron su adecuación con la versión antigua y no hayan completado el proceso, o incluso para las que deseen migrar a la versión actual.

[2] Xataka (2022) Disponible en: https://www.xataka.com/seguridad/ayuntamientos-navarra-vuelven-al-papel-estragos-ciberataque-que-dura-casi-dos-semanas (Consultada el 1 de abril de 2033)

[3] Las Provincias (2023) Disponible en: https://www.lasprovincias.es/sociedad/ciberataques-ayuntamientos-valencianos-20230207152213-nt.html (Consultada el 1 de abril de 2033)

[4] La Vanguardia (2021) Disponible en: https://www.lavanguardia.com/local/barcelona/20210122/6189766/veintena-ayuntamientos-atacados-ciberdelincuentes.html (Consultada el 1 de abril de 2033)

Este objetivo viene motivado por el hecho de que se hayan publicado muchas infografías[5] y resúmenes acerca del nuevo ENS, pero no exista una guía oficial de migración o actualización por parte del CCN. Las publicaciones de la nueva versión son escuetas, y mencionan las características del nuevo ENS, pero se limitan a enumerarlas sin llegar a compararlas con el ENS antiguo. ¿Se trata solo de un cambio de nomenclatura de los apartados? ¿Los controles del anexo que han cambiado implican nuevas medidas? ¿Cambia la metodología? Se tratará de dar respuesta a todas estas preguntas.

2. **Proveer uno de los primeros documentos de ejemplo para entidades locales siguiendo el nuevo ENS**, de modo que la comunidad universitaria, los ayuntamientos y sus proveedores, dispongan de ayuda extra a la hora de adecuar sus sistemas.

   Este objetivo viene motivado por la demora de actualización en muchas de las guías STIC, situación que lleva a los equipos de TI a aplazar las adecuaciones al ENS por estar en un momento de cambio.

   Adicionalmente, existen casos de ayuntamientos reales que han compartido públicamente los documentos de sus planes de adecuación, ya sea a través de charlas o ponencias, o directamente como ejercicio de transparencia, pero lamentablemente son todos contra la versión anterior del ENS.

3. **Identificar los principales escollos a la adecuación encontrados**, en busca de posibles causas de los bajos niveles de implantación actuales. De esta manera se podrían definir líneas de actuación encaminadas a facilitar la adopción del ENS y adecuación de los sistemas. Cabe destacar que la mayoría de las iniciativas existentes, se han orientado a reducir y simplificar los requisitos de seguridad, con ejemplos como µCeENS, o los perfiles de cumplimiento, los cuales, aunque son recientes, no han conseguido resultados inmediatos.

   Previo a la ejecución del proyecto, se barajan 3 posibles hipótesis: falta presupuestaria, desconocimiento de las herramientas disponibles o falta de priorización por no existir un régimen sancionador.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

El propio texto del ENS, en su preámbulo, contienen el siguiente texto:

"El ENS, cuyo ámbito de aplicación comprendía todas las entidades de las administraciones públicas, perseguía fundamentar la confianza en que los sistemas de información prestan sus servicios adecuadamente y custodian la información […], de forma que ***se facilite a los ciudadanos y a las administraciones públicas el ejercicio de sus derechos y el cumplimiento de sus obligaciones*** *a través de medios electrónicos."*

[5] Centro Criptológico Nacional (CCN) (2023) Disponible en: https://www.ccn-cert.cni.es/seguridad-al-dia/novedades-ccn-cert/11772-el-nuevo-ens-explicado-en-infografias.html (Consultada el 1 de junio de 2023)

Esta declaración tiene relación directa con el **Objetivo de Desarrollo Sostenible 16 de la ONU**, que analiza la importancia de disponer de unas instituciones sólidas para poder conseguir un entorno de paz y justicia. Concretamente, dos de sus metas, buscan:

- *"16.6 Crear a todos los niveles instituciones eficaces y transparentes que rindan cuentas"*
- *"16.10 Garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales"*

Las leyes nacionales y autonómicas en materia de transparencia delegan al ENS el aseguramiento de las 5 dimensiones de la seguridad de la información entre las que se encuentran la Disponibilidad, Integridad, Autenticidad y Trazabilidad, necesarias todas ellas para poder brindar información veraz, no manipulada y confiable, a la vez que requieren de sistemas siempre disponibles para garantizar el acceso continuo a la información.

Además, el nuevo ENS, en su artículo 30, introduce precisamente los nuevos perfiles de cumplimiento, los cuales facilitan una implantación particularizada y más **eficaz** en los ayuntamientos, ya que conociendo las dificultades que tienen estas pequeñas entidades locales y sus pocos recursos, ha personalizado algunos controles atendiendo a sus particularidades.

Por otro lado, cabe destacar que el ENS vela por la protección de la **confidencialidad** de la información, la quinta de las dimensiones de la seguridad que juega un papel crucial para garantizar la **privacidad de las personas**: los ayuntamientos tratan datos sobre servicios sociales como familias en riesgo de exclusión social, datos de discapacidades, solicitud de ayudas, o programas de apoyo a víctimas de violencia de género, cuya integridad y confidencialidad son esenciales para el bienestar de las personas.

Sin una adecuada protección, también pueden quedar comprometidos datos de **control medioambiental** dificultando la toma de decisiones, datos **económicos** fallando en la responsabilidad de administrar el dinero de los contribuyentes, o simplemente imposibilitando la **prestación de servicios básicos** que tienen encomendados.

Es por todo ello, que la implantación del ENS ayuda a los ayuntamientos a responder de la **responsabilidad social** que tienen con su ciudadanía y con el resto de la sociedad, la cual también queda recogida en el preámbulo del ENS:

[Acerca de las amenazas a las que están expuestas los sistemas] "*Todo ello afecta significativamente a un número cada vez mayor de entidades públicas y privadas, a sus cadenas de suministro, a los ciudadanos y, por ende, a la ciberseguridad nacional, lo que compromete el normal desenvolvimiento social y económico del país y el ejercicio de los derechos y libertades de los ciudadanos, como reconocen tanto la Estrategia de Ciberseguridad Nacional de 2013 como, particularmente, la Estrategia Nacional de Ciberseguridad 2019.*"

1.4. Enfoque y método seguido

La adecuación al ENS es un proyecto de envergadura que debe ser abordado descomponiendo el problema en diferentes fases y abordándolas mediante la consecución de pequeños hitos.

Para ello, existen 3 vías claramente diferentes que se exponen a continuación:

- El propio texto del ENS tiene una redacción y estructura muy práctica y contiene tres apartados principales a cubrir: principios básicos, requisitos mínimos y medidas de seguridad, por lo que es posible **abordar el ENS página a página** hasta conseguir la adecuación. Si bien puede parecer la opción más lógica, de seguirla es posible que algunos apartados de base, como la política de seguridad, no se aborden en fases tempranas con suficiente profundidad, dando pie a que no cumplan todos los requisitos esperados, a que se tomen decisiones posteriores basadas en una política incompleta, y a que se tengan que hacer excesivas correcciones.
- Utilizar la guía 802 de auditoría del ENS, para **preparar las respuestas a cada una de las preguntas que se realizarán el día de la auditoría**. Esta estrategia puede ser la vía más sencilla y directa de obtener la certificación, aunque no es la más responsable, ya que las decisiones que se tomen buscarán facilitar la certificación en vez de buscar los niveles de seguridad que los sistemas realmente necesitan, pudiendo dar como resultado una falsa sensación de seguridad y unos sistemas infravalorados.
- **Utilizar la guía 806 de adecuación al ENS**, que, a pesar de estar redactada para la versión anterior, indica de forma muy estructurada los pasos a seguir para adecuar nuestros sistemas.

Ante la falta de una guía actualizada, se ha optado por realizar este trabajo siguiendo un enfoque mixto siguiendo la estructura de la guía 806 de adecuación al ENS anterior, con el texto del nuevo ENS.

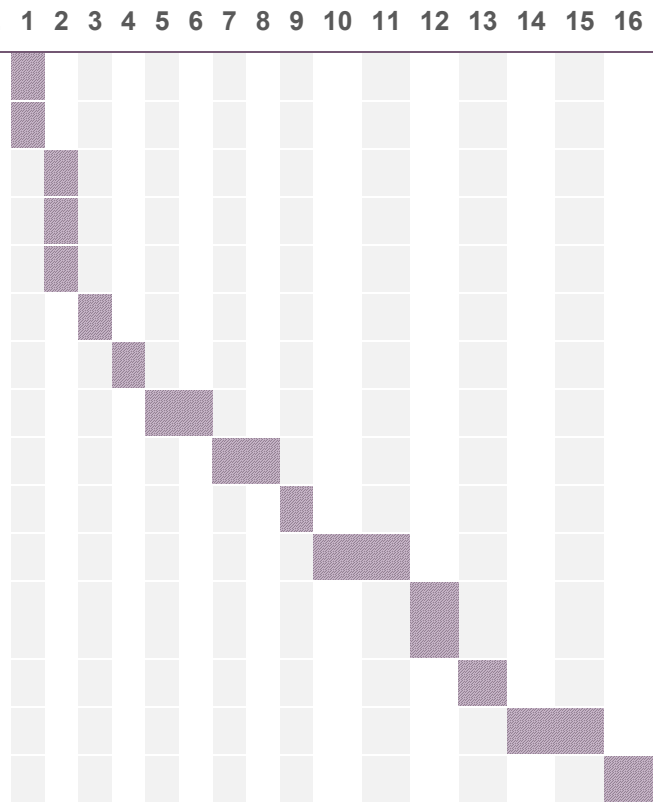
Dicha guía define los siguientes pasos naturales, cada uno de los cuales se ampliará en el apartado correspondiente:

- Política de seguridad de la información y normativa interna.
- Identificar servicios e información y categorizar sistemas
- Nivel de seguridad y categoría de seguridad.
- Análisis de riesgos
- Declaración de aplicabilidad
- Análisis diferencial
- Plan de mejora de la seguridad
- Declaración de conformidad o auditoría de certificación

1.5. Planificación del Trabajo

A continuación, se muestra la planificación y duración estimada de las tareas identificadas.

ACTIVIDAD	INICIO	DURAC.
Contexto y justificación	1	1
Objetivos	1	1
Impacto en sostenibilidad	2	1
Enfoque y método	2	1
Planificación	2	1
Política de seguridad	3	1
Valoración de sistemas	4	1
Análisis de riesgos	5	2
Análisis diferencial de controles	7	2
Plan de acciones	9	1
Ejecución de acciones	10	2
Documentación acciones futuras	12	1
Conclusiones	13	1
Maquetado final	14	2
Presentación en video	16	1



1.6. Breve sumario de productos obtenidos

- Resumen del proceso de adecuación
- Ejemplo completo de política de seguridad
- Ejemplo completo de valoración de sistemas
- Ejemplo completo de análisis de riesgos sin necesidad de herramientas, usando MAGERIT
- Ejemplo completo de declaración de aplicabilidad con valoración de la madurez y la implantación
- Listado de tareas periódicas para seguimiento del ENS
- Listado de principales novedades del ENS y posibles escoyos para su implantación
- Ejemplo de política de control de accesos
- Ejemplo de implantación de sistema de centralización de logs y protección de los mismos

2 Ejecución

El primer paso será hacer una pequeña introducción con el **contexto y contexto TIC** de CiudadX, que ayudará a comprender tanto la estructura y funcionamiento del ayuntamiento, como el alcance y complejidad de la implantación. Posteriormente, tal y como se ha indicado en el apartado 1.4, se va a utilizar como esquema para todo el proceso la *Guía CCN-STIC 806 Plan de Adecuación del ENS*, cada uno de cuyos pasos da nombre a un título del presente apartado.

2.1 La ciudad

Antes de empezar con los detalles del proceso de adecuación, es necesario ofrecer más contexto acerca del Ayuntamiento de CiudadX, sus servicios y su infraestructura TIC.

La ciudad cuenta con cerca de 25.000 habitantes agrupados en un único casco urbano con una superficie urbana de aproximadamente 2 km^2.

Durante los últimos años ha experimentado un crecimiento importante en su población y por lo tanto en la recaudación (ingresos), infraestructura necesaria y servicios prestados.

2.2 Contexto TIC

Con motivo del mencionado crecimiento, en pocos años ha pasado de delegar gran parte de la gestión TIC en la diputación, a crear un pequeño CPD para albergar la creciente demanda de servicios, para finalmente migrar prácticamente toda la gestión de sus sistemas a infraestructuras de terceros en modo IaaS o SaaS.

La **infraestructura** TIC actual es la siguiente:

Disponen de un **pequeño CPD** en el ayuntamiento con menos de una docena de servidores para servicios locales:

- Controlador del dominio, que hace también las funciones de servidor de impresión, DNS externo, gestión de identidades, y carpetas compartidas.
- Servidor de los administradores TIC, con herramientas de inventariado de equipos y software, control NAC, monitorización, consolas para acceder a electrónica de red, software de gestión de contraseñas, etc.
- Servidor de bases de datos.
- Servidor con la consola de administración del antivirus.
- Cabina de discos donde vuelcan copias de seguridad de sus datos locales y externalizados.
- Electrónica de red para la conexión a Internet, servidor de VPN, detector de intrusiones y conectividad LAN.

El ayuntamiento dispone de **30 puestos de trabajo** normalizados, los cuales se plataforman con una plantilla base que incluye el sistema operativo y las herramientas ofimáticas de uso común. Estos equipos son tanto para el personal administrativo, informática, así como ordenanzas y cargos electos. Forman parte de un directorio activo que administra el personal funcionario y disponen de un antivirus controlado mediante una consola centralizada. Estos equipos se conectan entre si mediante red cableada o una red Wifi dedicada a la que no tienen acceso ciudadanos o externos.

Las **herramientas y aplicaciones** necesarias para el funcionamiento del ayuntamiento (gestiones internas, gestión urbanística, padrón, tributos, contratación y sede electrónica) se prestan en dos modalidades:

- Las que han sido **desarrolladas a medida,** se ejecutan en un proveedor *cloud* en modo ***IaaS***, tienen todas una arquitectura similar (Java principalmente mediante acceso web), y los servidores son administrados por el personal del ayuntamiento con la ayuda de una empresa de servicios. Las empresas desarrolladoras no disponen de acceso a estos entornos. El acceso a dichas aplicaciones se filtra mediante reglas de firewall, de modo que solo son accesibles desde las direcciones IP del ayuntamiento, incluida la VPN.
  Los datos de todas estas aplicaciones se almacenan en una gran base de datos centralizada, administrada por el personal del ayuntamiento y de la cual se hace una copia diaria en las instalaciones del ayuntamiento.
- Las **herramientas comerciales** destinadas a la gestión de ayuntamientos son prestadas por los proveedores en modo ***SaaS***, siendo alojadas en las dependencias de los proveedores, o en otros proveedores *cloud*, cuya administración está delegada. En estos casos, no se dispone de acceso de administración sobre los servidores, aunque existen contratos que regulan la posible exportación de los datos si hubiera un cese del contrato. El acceso a dichas aplicaciones también se filtra mediante reglas de firewall, de modo que solo son accesibles desde las direcciones IP del ayuntamiento. Estas herramientas disponen de sus propias bases de datos, aunque vuelcan diariamente una copia de los datos a la cabina del ayuntamiento.

La conexión a **Internet** está contratada con un importante proveedor de internet que es quien también se encarga de prestar servicios AntiDDoS y de la interconexión con la red SARA[6] (Sistema de Aplicaciones y Redes para las Administraciones). Se dispone de un cortafuegos en dicha salida.

El **correo electrónico** está externalizado en un importante proveedor, que además proporciona la *suite* **ofimática** con almacenamiento de trabajo online que se utiliza a modo de repositorio de documentación.

La **página web** municipal está también en un proveedor externo, es gestionada directamente por el mismo personal del ayuntamiento que gestiona los perfiles públicos de las **redes sociales**, mientras que es administrado por el personal TIC funcionario. Contiene un enlace a la sede electrónica, pero son sistemas diferentes.

Aparte de las aplicaciones y servicios TIC habituales en un ayuntamiento, CiudadX cuenta con los siguientes servicios particulares:

- **Plataforma de gestión de incidencias:** servicio que unifica la comunicación entre ciudadanos, administración y proveedores para todo tipo de incidencias y peticiones relacionadas con la población. Permite reportar problemas en la vía pública, en servicios TIC, edificios o instalaciones, incidencias de tráfico, asuntos de jardinería-alumbrado-alcantarillado-incendio-emergencias municipal entre otros, así como asignarlos al personal que debe evaluarlos o resolverlos, y llevar el seguimiento de estos. Muchos servicios y aplicaciones municipales utilizan esta interfaz para gestionar las peticiones internas de servicio, como la gestión de accesos, las incidencias TIC o las solicitudes de nuevas aplicaciones.
- **Geoportal**: servicio de cartografía y geolocalización de activos municipales y puntos de interés. Además de ofrecer información de interés a ciudadanos, sirve de complemento para la aplicación de gestión de incidencias.

[6] Red SARA. Gobierno de España (2023) Disponible en: https://administracionelectronica.gob.es/ctt/redsara/masmas#.ZDWVJPZBxD8 (Consultada el 11 de abril de 2023.

- **APP móvil:** aplicación para dispositivos móviles que permite acceder a la reserva de edificios y servicios municipales, contenido de redes sociales e información web, así como información divulgativa de iniciativas y actividades municipales.

2.1 Política de seguridad

Según el propio ENS, "*la política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta*", siendo uno de los pilares del resto de la adecuación, además de un documento de obligada cumplimentación.

Para ayudar en el proceso, en 2011 el CCN publicó la *"**Guía de seguridad ccn-stic-805 Política de seguridad de la Información**"* que está dedicada en exclusiva a la redacción de la política, la cual es una base excelente para este apartado.

Si bien el apartado de la política en el nuevo ENS ha tomado relevancia al pasar de ser una medida de seguridad a disponer de un capítulo completo, los cambios introducidos solo aplican a la forma de aprobar formalmente la política por diferentes tipos de organismos, sin afecta al caso concreto de los ayuntamientos.

Lo que sí que se menciona es que debe redactarse con el foco en los principios básicos del nuevo ENS, por lo que se incorporarán a la plantilla facilitada por el CCN cuando corresponda, pero sin llegar a sustituir a los procedimientos correspondientes (de organización, análisis de riesgos, gestión de personal, etc.).

La política creada puede consultarse en el **Anexo I** del presente documento.

2.2 Identificar servicios e información y categorizar sistemas

Una vez definida la política, el siguiente paso es identificar tanto los ***servicios*** que ofrece el ayuntamiento, como las ***unidades de información*** (bases de datos, conjuntos de datos, ficheros electrónicos, repositorios documentales, etc.) que estos servicios utilizan.

La combinación de uno o varios servicios y una o varias informaciones, dará lugar a un ***sistema de información***, en adelante sistema, sobre el cual se aplicarán diferentes medidas de seguridad según los requisitos que los responsables hayan definido.

Ya que este apartado es **muy** relevante y los conceptos serán repetidos durante todo el documento, se enfatizan mediante la siguiente figura:

_n_ servicios + _n_ unidades de información

=

sistema de información

- Siendo un **servicio**, por ejemplo, la acción de poder acceder al padrón junto con todos los activos necesarios para que la acción se pueda realizar (aplicación, comunicaciones, personal, servidores)
- Siendo una **unidad de información** una base de datos, una hoja de cálculo, cualquier fichero electrónico, o incluso documentos en papel

Figura 1 - Servicios e información

Nótese el énfasis en servicios, unidades de información y sistema: los 3 conceptos son detallados en el apartado "glosario".

El texto del ENS lo explica de la siguiente manera: "*La categoría de seguridad de un sistema de información modulará el equilibrio entre la importancia de la información que maneja y los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.*

La determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, siguiendo el procedimiento descrito en el anexo I"

Respecto a los servicios, tal y como recomienda el anexo II de la guía 883 de adecuación, la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (LBRL), establece que ayuntamientos como el de CiudadX, debido al tamaño de su población, está obligado a cubrir las siguientes competencias:

- Alumbrado público
- Cementerio
- Recogida y tratamiento de residuos y limpieza viaria
- Abastecimiento domiciliario de agua potable y alcantarillado
- Acceso a los núcleos de población y pavimentación de las vías públicas.
- Parque público, biblioteca pública e instalaciones deportivas públicas
- Protección civil
- Evaluación e información de situaciones de necesidad social y la atención inmediata a personas en situación o riesgo de exclusión social
- Prevención y extinción de incendios
- Urbanismo

Existen otras muchas como el mantenimiento de los centros de salud, o la vigilancia de la escolarización obligatoria, de las cuales se han incluido en el alcance aquellas que tienen una dependencia directa de sistemas de información, concretamente las siguientes:

- Padrón de habitantes
- Gestión de tributos

- Gestión y promoción de la cultura, actividades juveniles, deportes y participación ciudadana
- Sede electrónica

Por último, se han incluido los siguientes servicios ajenos a la Ley 7/1985 que CiudadX proporciona a sus habitantes y tienen fuerte dependencia de las TIC:

- Geoportal: portal con datos localización de mobiliario urbano, cartografía, edificios municipales, y puntos de interés. Es utilizado por la página web municipal, el servicio de gestión de incidencias, proveedores, y ciudadanos para acceder a información del municipio.
- Sistema de gestión de incidencias municipal: sistema centralizado de peticiones y notificación de incidencias. Permite a los ciudadanos solicitar reparaciones en mobiliario urbano o notificar deficiencias en la vía pública, y a los propios empleados del ayuntamiento a crear, distribuir y gestionar peticiones de servicio a ellos mismos y a los proveedores.
- Web, APP y redes sociales: servicios de distribución de información a la ciudadanía de forma cercana y sencilla.

Con todo ello, el responsable de cada uno de los servicios de CiudadX deberá valorarlos siguiendo el anexo I del ENS, como se ha hecho de forma ficticia en la siguiente tabla, donde las columnas DICAT, corresponden a Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad.

Nótese que siguiendo la Guía 803 de valoración de sistemas, en los **servicios**, únicamente se valora la **disponibilidad** de estos, ya que el **resto de las dimensiones** aplican a la **información** que utilizan estos servicios y ha de ser valorada por el responsable del dato. Esta distinción queda patente en el siguiente fragmento de la guía:

*"Habiendo identificado previamente los servicios prestados por la entidad, sujetos al cumplimiento del ENS, conviene comenzar la valoración por los activos de tipo **información** utilizados por tales servicios, valorando, en este orden: **confidencialidad, integridad, trazabilidad, autenticidad** y, si fuera relevante, disponibilidad. Es frecuente que la disponibilidad no sea un atributo relevante de la información y quede sin adscribir a ningún nivel.*

*Conviene seguir con los activos de tipo **servicio**, valorando para los mismos la **disponibilidad**. Los requisitos en materia de confidencialidad, integridad, trazabilidad y autenticidad suelen venir impuestos por los tipos de información que maneja cada servicio, asumiendo los establecidos en el párrafo anterior."*

Servicio	Descripción	D	I	C	A	T
Aplicación de padrón	Gestión interna del padrón municipal	B	N/A	N/A	N/A	N/A
Gestión de incidencias locales	Gestión y asignación de incidencias locales a proveedores y personal propio	M	N/A	N/A	N/A	N/A
Gestión de tributos	Gestión interna de los tributos locales	A	N/A	N/A	N/A	N/A
Gestión de iniciativas de cultura, juventud, deportes y participación ciudadana	Aplicación de gestión de iniciativas de cultura, juventud, deportes y participación ciudadana	B	N/A	N/A	N/A	N/A
Gestión de datos del geoportal	Aplicación interna para añadir, modificar y gestionar puntos de interés del geoportal	M	N/A	N/A	N/A	N/A
Redes sociales y portales web	Redes sociales y la propia web municipal	B	N/A	N/A	N/A	N/A
Gestión urbanística	Aplicación interna de tramitación de expedientes urbanísticos	M	N/A	N/A	N/A	N/A
Gestión de espacios públicos y reservas	Aplicación interna de gestión de espacios públicos	B	N/A	N/A	N/A	N/A
Gestión de contratación	Aplicación interna para las gestiones de contratación y seguimiento de proveedores	M	N/A	N/A	N/A	N/A
Gestión del cementerio	Aplicación interna del cementerio municipal	B	N/A	N/A	N/A	N/A
Gestión de servicios sociales	Aplicación interna de gestión de los servicios sociales municipales	A	N/A	N/A	N/A	N/A
Servicios de la sede electrónica	-Consulta y gestiones del padrón. -Consulta y gestiones del cementerio -Plataforma de contratación Intranet de RRHH -Comunicación de incidencias locales -Pago de tributos -Trámites urbanísticos -Solicitud y gestión de servicios sociales -Consulta de expedientes y trámites, registro de entrada/salida electrónico	M	N/A	N/A	N/A	N/A

APP móvil municipal	-Comunicación de incidencias locales -Publicidad de iniciativas culturales, deportivas, juveniles y de participación ciudadana -Consulta del geoportal -Reserva de edificios públicos y espacios -Consulta de la actualidad municipal	B	N/A	N/A	N/A	N/A

Tabla 1 Identificación y valoración de servicios

B Bajo M Medio A Alto N/A No aplica

Como se puede apreciar, el responsable de servicio de tributos ha valorado la disponibilidad de su servicio como *alta*, ya que la recaudación es vital para que el ayuntamiento pueda conseguir sus objetivos, además de que el no dejar a un ciudadano abonar tasas pendientes, podría desencadenar en procesos legales difícilmente reparables.

Por otro lado, la gestión de servicios sociales también ha sido categorizada como *alta* ya que trabaja con colectivos vulnerables, y la pronta atención es vital para algunos casos como la atención a víctimas de violencia de género o a la atención a menores con necesidades especiales, con el consiguiente riesgo para sus vidas o integridad.

Los servicios categorizados con nivel *medio* se deben principalmente a que, aunque son necesarios para alcanzar los objetivos del Ayuntamiento de CiudadX, existen métodos alternativos para prestar dichos servicios o se podría encolar su prestación hasta 1 día.

Por último, los servicios categorizados con nivel *bajo* responden a la existencia de mecanismos sencillos para su sustitución, posibilidad de servirlos por medios alternativos y a no atender a necesidades urgentes de la ciudadanía ni de la gerencia del ayuntamiento.

De igual modo, se ha identificado las siguientes unidades de información con la correspondiente valoración por parte de su responsable:

Servicio	Descripción	D	I	C	A	T
Datos del padrón	Datos de los empadronados del municipio con fines de censo electoral, histórico y estadístico	N/A	A	B	A	A
Datos de incidencias locales	Datos de las incidencias locales que nutren diferentes aplicaciones para el mantenimiento y gestión de infraestructuras y servicios del municipio	N/A	M	B	B	B
Datos de tributos	Datos sobre la recaudación de impuestos y tasas	N/A	M	M	M	M
Datos de iniciativas de cultura, juventud, deportes y participación ciudadana	Datos de acciones de difusión y fomento de actividades generales: datos de asistentes, alcance, organización de eventos e iniciativas, etc.	N/A	B	B	B	B
Datos del geoportal	Datos sobre coordenadas GPS de mobiliario urbano, infraestructuras y otros puntos de interés del municipio para varias gestiones y servicios	N/A	M	B	B	B
Datos de redes sociales y portales web	Información destinada a la página corporativa y las redes sociales	N/A	M	B	M	B
Datos de urbanismo	Datos de ordenación del terreno y trámites urbanísticos	N/A	A	B	M	A
Datos de espacios públicos y reservas	Datos sobre infraestructuras municipales y la gestión de estos: reservas, agenda, gestiones, etc.	N/A	B	B	B	B
Datos de contratación y personal	Datos sobre el personal, propio y externo, así como de sus relaciones contractuales con el municipio, incluidas empresas y proveedores	N/A	M	M	M	M
Datos del cementerio	Datos sobre la gestión del cementerio y defunciones	N/A	A	B	M	M
Datos de servicios sociales	Datos de las solicitudes de prestación de servicios sociales a colectivos vulnerables	N/A	A	A	A	A
Datos de la sede electrónica, archivo, expedientes y registro de entrada y salida	Datos del archivo municipal y trámites administrativos, sean online o presenciales	N/A	A	A	A	A

Tabla 2 Identificación y valoración de información

B Bajo M Medio A Alto N/A No aplica

En este caso, han sido varias las dimensiones marcadas como de nivel alto:

- La modificación, falsedad, o falta de trazabilidad sobre los datos del **padrón**, podrían, llegado el momento, desencadenar el rechazo de ayudas sociales o la

imposibilidad de ejercer el derecho al voto, por lo que el responsable las la valorado como *alto*.

- Los datos de **urbanismo**, cuya manipulación puede ser posible objetivo de falsificación o fraude, han marcado como *alta* su integridad y trazabilidad, de modo que cualquier modificación sobre ellos, quede trazada y sea demostrable en caso de sospecha.
- La integridad de los datos del **cementerio** se ha marcado como *alta*, ya que un fallo o dato corrupto en los mismos podría desencadenar importantes daños morales a los familiares de los fallecidos. Dada la sensibilidad de dicha situación y por compromiso con las familias de CiudadX, se ha fijado dicho nivel.
- Los responsables de los datos de los **servicios sociales**, conocedores del daño irreparable que podría sufrir la ciudadanía, han decidido establecer requisitos altos de confidencialidad para evitar filtraciones, así como de integridad, trazabilidad y autenticidad para evitar tanto la asignación fraudulenta de beneficios, como la posible retirada injusta de servicios a ciudadanos necesitados.
- Los datos de la sede electrónica y trámites han sido categorizados como *altos*, ya que cumplir con los más altos requisitos de seguridad es un requisito de la ley del procedimiento administrativo común, y su malfuncionamiento, inconsistencia, o filtración, podría poner en duda la confianza en la administración pública por parte de la ciudadanía.

El nivel *medio* se ha asignado a aquellas dimensiones cuya vulneración supondría inconvenientes, pero no impedimentos para que el ayuntamiento pudiera ofrecer sus servicios a la ciudadanía, mientras que los de nivel bajo se han aplicado a aquellas, que tendrían fácil subsanación.

2.3 Nivel de seguridad y categoría de seguridad

A la vista de la valoración realizada por los responsables de los servicios y la información, de la tipología de estos, y atendiendo a que existe gran discrepancia entre los niveles de cada uno de ellos, se ha optado por crear 4 sistemas independientes, de modo que se flexibilizará y particularizará la gestión de la seguridad para cada uno de ellos:

Sistema 1. Administración y tramitación	D	I	C	A	T
Aplicación de padrón	B	N/A	N/A	N/A	N/A
Datos del padrón.	N/A	A	B	A	A
Gestión de tributos	A	N/A	N/A	N/A	N/A
Datos de tributos	N/A	M	M	M	M
Gestión urbanística	M	N/A	N/A	N/A	N/A
Datos de urbanismo	N/A	A	B	M	A
Gestión de contratación	M	N/A	N/A	N/A	N/A
Datos de contratación y personal	N/A	M	M	M	M
Servicios de la sede electrónica	M	N/A	N/A	N/A	N/A
Datos de la sede electrónica, archivo, expedientes y registro de entrada y salida	N/A	A	A	A	A
NIVEL MÁXIMO	**A**	**A**	**A**	**A**	**A**

Tabla 3 Valoración sistema 1

B Bajo M Medio A Alto N/A No aplica

Sistema 2. Gestión urbana	D	I	C	A	T
Gestión de incidencias locales	M	N/A	N/A	N/A	N/A
Datos de incidencias locales	N/A	M	B	B	B
Gestión de datos del geoportal	M	N/A	N/A	N/A	N/A
Datos del geoportal	N/A	M	B	B	B
Gestión del cementerio	B	N/A	N/A	N/A	N/A
Datos del cementerio	N/A	A	B	M	M
NIVEL MÁXIMO	**M**	**A**	**B**	**M**	**M**

Tabla 4 Valoración sistema 2

B Bajo M Medio A Alto N/A No aplica

Sistema 3. Bienestar ciudadano	D	I	C	A	T
Gestión de iniciativas de cultura, juventud, deportes y participación ciudadana	B	N/A	N/A	N/A	N/A
Datos de iniciativas de cultura, juventud, deportes y participación ciudadana	N/A	B	B	B	B
Redes sociales y portales web	B	N/A	N/A	N/A	N/A
Datos de redes sociales y portales web	N/A	M	B	M	B
Gestión de espacios públicos y reservas	B	N/A	N/A	N/A	N/A
Datos de espacios públicos y reservas	N/A	B	B	B	B
APP móvil municipal	B	N/A	N/A	N/A	N/A
NIVEL MÁXIMO	**B**	**M**	**B**	**M**	**B**

Tabla 5 Valoración sistema 3

B Bajo M Medio A Alto N/A No aplica

Sistema 4. Servicios sociales	D	I	C	A	T
Gestión de servicios sociales	A	N/A	N/A	N/A	N/A
Datos de servicios sociales	N/A	A	A	A	A
NIVEL MÁXIMO	**A**	**A**	**A**	**A**	**A**

Tabla 6 Valoración sistema 4

B Bajo M Medio A Alto N/A No aplica

2.4 Análisis de riesgos

Del apartado anterior, se ha obtenido una lista de aquellos sistemas, (recordemos, servicios + informaciones), que el ayuntamiento considera más relevantes o sensibles, obteniendo una "perspectiva del negocio".

A continuación, y siguiendo la guía de adecuación 806 de adecuación, el siguiente paso será abordar el análisis de riesgos TIC, donde se analizará qué amenazas sobre los componentes tecnológicos pueden impedir que los sistemas funcionen según los criterios establecidos por sus responsables.

Este análisis en dos fases, donde se separa el negocio de la tecnología, es necesario para asegurar que las decisiones de TI están alienadas con los objetivos de la organización.

Para este análisis de riesgos TIC, se ha seleccionado la metodología MAGERIT versión3[7] del Consejo Superior de Administración Electrónica, que se define así según la referencia anterior:

"MAGERIT es una metodología de carácter público que puede ser utilizada libremente y no requiere autorización previa. Interesa principalmente a las entidades en el ámbito de aplicación del Esquema Nacional de Seguridad (ENS) para satisfacer el principio de la gestión de la seguridad basada en riesgos, así como el requisito de análisis y gestión de riesgos, considerando la dependencia de las tecnologías de la información para cumplir misiones, prestar servicios y alcanzar los objetivos de la organización."

Consta de 3 libros, de los cuales utilizaremos el primero para seguir la metodología, y el segundo para seleccionar el catálogo de activos, amenazas y salvaguardas.

Así pues, los pasos a seguir serán los siguientes:

- Identificación de activos y dependencias
- Identificación de amenazas, probabilidad, impacto y riesgo potencial
- Identificación de salvaguardas
- Cálculo del riesgo residual y aceptación formal

2.4.1 Identificación de activos y dependencias

Se han identificado los principales **activos** del Ayuntamiento de CiudadX que influyen en el funcionamiento de los sistemas TIC, se han **clasificado** según el catálogo del Libro II de MAGERIT, se han relacionado con **los sistemas a los que prestan servicio** (y que por tanto dependen de ellos) y se ha establecido el **porcentaje estimado de dependencia**. Esta valoración de dependencia se ha establecido según la necesidad de que las dimensiones de la seguridad del activo TIC no se vean comprometidas para que el sistema pueda seguir funcionando. Los valores *alto* indican que el activo es necesario para la prestación, mientras que los *bajo* pueden deberse a la existencia de medios alternativos, o a la no necesidad de que el activo esté operativo.

Activo	Sistemas a los que da soporte	% de dependencia
Activos de tipo Software		
Sistemas Operativos Servidores	Todos	100%
Windows + ofimática, correo, antivirus	Todos	100%
Mantenimiento sistemas: monitorización, copias de seguridad, inventario, SO servers	Todos	100%
Gestiones internas ayuntamiento: fichaje, RRHH, intranet, etc.	Todos	10%
Carpetas compartidas	Todos	25%
Apache, PHP y JavaScript (Web municipal)	Todos	100%
Tomcat y Java	Todos	100%
Base de datos central	Todos	100%
Gestión urbanística	Sist. Administración y tramitación	25%
Aplicación padrón	Sist. Administración y tramitación	25%
Gestión de tributos	Sist. Administración y tramitación	25%
Gestión contratación	Sist. Administración y tramitación	25%
Sede electrónica, archivo, expedientes y registro	Sist. Administración y tramitación	50%
Gestión de incidencias	Sistema Gestión urbana	75%
Gestión geoportal	Sistema Gestión urbana	50%
Gestión cementerio	Sistema Gestión urbana	25%
Gestión cultura, deportes, juventud y participación	Sistema Gestión urbana	25%
APP móvil	Sistema Bienestar Ciudadano	20%
Gestión espacios públicos	Sistema Bienestar Ciudadano	25%
Redes sociales	Sistema Bienestar Ciudadano	20%
Gestión servicios sociales	Sistema Servicios Sociales	100%
Activos de tipo Hardware		
Servidor de directorio activo	Todos	80%
Puestos de trabajo	Todos	80%
Dispositivos móviles corporativos	Todos	25%

Cabina de discos para copias de seguridad	Todos	10%
Activos de tipo Comunicaciones		
Red LAN interna	Todos	90%
Electrónica de red (routers/switches)	Todos	90%
Telefonía	Todos	25%
Conexiones a red SARA	Sistema Servicios sociales	90%
Conexiones a red SARA	Sist. Administración y tramitación	90%
Activos de tipo Elementos Auxiliares		
Aire acondicionado CPD	Todos	90%
Discos duros externos	Todos	5%
Impresoras	Todos	10%
SAI / Grupo electrógeno	Todos	10%
Activos de tipo servicios auxiliares		
Empresa mantenimiento HW	Todos	50%
Conexión WAN	Todos	75%
IaaS cloud	Todos	90%
SaaS cloud	Todos	90%
Empresa desarrollo de aplicaciones	Todos	50%
Empresa soporte a sistemas	Todos	50%
Activos de tipo Instalaciones		
CPD propio	Todos	90%
Armario comunicaciones	Todos	90%
Edificio Ayuntamiento	Todos	90%
Activos de tipo Personal		
Personal funcionario	Todos	100%
Personal externo	Todos	80%

Tabla 7 Activos y dependencias

2.4.2 Identificación de amenazas y cálculo del riesgo

Siguiendo con la metodología MAGERIT (libro I), para cada se han seleccionado las amenazas del catálogo (libro II) más relevantes, tanto por probabilidad como por impacto.
Para cada una de estas amenazas, se ha establecido una **probabilidad** (P) de materialización, un **impacto** (I) según la degradación que supondría en el activo, para en pasos siguientes, calcular el **riesgo absoluto** mediante la fórmula R=P*I.

Ya que se trata de una valoración subjetiva, se han utilizado valores cualitativos con 5 niveles, desde el 1 al 5, siendo equiparables a Muy bajo (1), Bajo (2), Medio (3), Alto (4) y Muy Alto (5), siguiendo la siguiente matriz para el cálculo del riesgo:

Probabilidad					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
			Impacto		

Tabla 8 Matriz de cálculo del riesgo absoluto

También se ha trasladado a la tabla la lista de los **sistemas** a los que puede afectar la materialización de una amenaza para así poder aplicarle un factor **multiplicador** del 25% si el sistema es de **nivel medio** o del 50% si es de **nivel alto**, según los apartados anteriores.

De forma similar, se han incorporado los **porcentajes de dependencia** de cada activo con cada servicio, calculados en el apartado anterior.

Aplicando ambos porcentajes al riesgo absoluto, obtenemos el valor final del riesgo (riesgo repercutido).

El primer resultado de la tabla se interpretaría de la siguiente manera:

*"El nivel de riesgo de que se comprometa **cualquier sistema** y sus servicios por que un **administrador cometa un error**, es de **12 puntos**."*

Activo	Amenaza	Probabilidad	Impacto	Riesgo absoluto	Sistemas a los que afecta	Multiplicador por dependencias	Multiplicador por criticidad	Riesgo repercutido
Sistemas Operativos Servidores								
	E.2 Errores del administrador	2	4	8	Todos	100%	150%	12
	E.20 Vulnerabilidades	3	5	15	Todos	100%	150%	22,5
	A.4 Manipulación de la configuración	1	5	5	Todos	100%	150%	7,5
	A.8 Difusión de software dañino	2	5	10	Todos	100%	150%	15
	A.5 Suplantación del usuario	2	5	10	Todos	100%	150%	15
Windows + ofimática, correo, antivirus								
	E.1 Errores de los usuarios	3	2	6	Todos	100%	150%	9
	E.2 Errores del administrador	2	3	6	Todos	100%	150%	9
	E.20 Vulnerabilidades	2	3	6	Todos	100%	150%	9
	A.4 Manipulación de la configuración	2	3	6	Todos	100%	150%	9
	A.5 Suplantación del usuario	3	4	12	Todos	100%	150%	18
	A.8 Difusión de software dañino	2	4	8	Todos	100%	150%	12
	A.11 Acceso no autorizado	2	5	10	Todos	100%	150%	15
	A.30 Ingeniería Social	2	4	8	Todos	100%	150%	12
Mantenimiento sistemas: monitorización, backup, etc.								
	E.2 Errores del administrador	1	3	3	Todos	100%	150%	4,5
	E.20 Vulnerabilidades	3	4	12	Todos	100%	150%	18
	A.3 Manipulación de los logs	2	4	8	Todos	100%	150%	12
	A.4 Manipulación de la configuración	2	4	8	Todos	100%	150%	12
	A.8 Difusión de software dañino	1	4	4	Todos	100%	150%	6
	A.11 Acceso no autorizado	1	5	5	Todos	100%	150%	7,5
Gestiones internas ayuntamiento: fichaje, RRHH, intranet, etc.								
	E.1 Errores de los usuarios	2	2	4	Todos	10%	150%	0,6
	E.2 Errores del administrador	1	3	3	Todos	10%	150%	0,45
	E.7 Deficiencias en la organización	3	2	6	Todos	10%	150%	0,9
	E.20 Vulnerabilidades	1	3	3	Todos	10%	150%	0,45
	A.5 Suplantación del usuario	3	3	9	Todos	10%	150%	1,35
	A.11 Acceso no autorizado	3	3	9	Todos	10%	150%	1,35
Carpetas compartidas								

E.1 Errores de los usuarios	3	3	9	Todos	25%	150%	3,375
E.2 Errores del administrador	1	3	3	Todos	25%	150%	1,125
E.20 Vulnerabilidades	2	4	8	Todos	25%	150%	3
A.8 Difusión de software dañino	2	4	8	Todos	25%	150%	3
A.11 Acceso no autorizado	1	3	3	Todos	25%	150%	1,125
Apache, PHP y JavaScript (portal web)							
E.2 Errores del administrador	1	4	4	Todos	100%	150%	6
E.20 Vulnerabilidades	3	4	12	Todos	100%	150%	18
E.21 Errores de mantenimiento	2	3	6	Todos	100%	150%	9
A.11 Acceso no autorizado	1	2	2	Todos	100%	150%	3
A.22 Manipulación de programas	2	3	6	Todos	100%	150%	9
A.24 Denegación de servicio	2	3	6	Todos	100%	150%	9
Tomcat y Java (aplicaciones internas)							
E.2 Errores del administrador	1	4	4	Todos	100%	150%	6
E.7 Deficiencias en la organización	1	4	4	Todos	100%	150%	6
E.19 Fugas de información	2	4	8	Todos	100%	150%	12
E.20 Vulnerabilidades	3	4	12	Todos	100%	150%	18
A.11 Acceso no autorizado	1	4	4	Todos	100%	150%	6
A.22 Manipulación de programas	2	4	8	Todos	100%	150%	12
Base de datos central							
A.3 Manipulación de los logs	1	3	3	Todos	100%	150%	4,5
A.5 Suplantación del usuario	1	3	3	Todos	100%	150%	4,5
A.6 Abuso de privilegios de acceso	2	4	8	Todos	100%	150%	12
A.11 Acceso no autorizado	1	5	5	Todos	100%	150%	7,5
A.18 Destrucción de la información	2	5	10	Todos	100%	150%	15
A.19 Divulgación de información	2	5	10	Todos	100%	150%	15
Gestión urbanística							
A.3 Manipulación de los logs	2	5	10	S1 Administ	25%	150%	3,75
A.6 Abuso de privilegios de acceso	1	5	5	S1 Administ	25%	150%	1,875
A.15 Manipulación deliberada de la información	1	5	5	S1 Administ	25%	150%	1,875
A.29 Extorsión	1	5	5	S1 Administ	25%	150%	1,875
Aplicación padrón							

A.3 Manipulación de los logs	1	5	5	S1 Administ	25%	150%	1,875
A.6 Abuso de privilegios de acceso	1	5	5	S1 Administ	25%	150%	1,875
A.15 Manipulación deliberada de la información	1	5	5	S1 Administ	25%	150%	1,875
Gestión de tributos							
A.3 Manipulación de los logs	1	5	5	S1 Administ	25%	150%	1,875
A.6 Abuso de privilegios de acceso	1	5	5	S1 Administ	25%	150%	1,875
A.15 Manipulación deliberada de la información	1	5	5	S1 Administ	25%	150%	1,875
A.24 Denegación de servicio	1	3	3	S1 Administ	25%	150%	1,125
Gestión contratación							
A.6 Abuso de privilegios de acceso	1	4	4	S1 Administ	25%	150%	1,5
A.11 Acceso no autorizado	1	4	4	S1 Administ	25%	150%	1,5
A.22 Manipulación de programas	1	4	4	S1 Administ	25%	150%	1,5
A.29 Extorsión	1	5	5	S1 Administ	25%	150%	1,875
Sede electrónica, archivo, expedientes y registro							
A.3 Manipulación de los logs	1	5	5	S1 Administ	50%	150%	3,75
A.5 Suplantación del usuario	2	4	8	S1 Administ	50%	150%	6
A.11 Acceso no autorizado	2	4	8	S1 Administ	50%	150%	6
A.13 Repudio	2	4	8	S1 Administ	50%	150%	6
A.24 Denegación de servicio	2	3	6	S1 Administ	50%	150%	4,5
Gestión de incidencias							
E.1 Errores de los usuarios	3	3	9	S2 G.Urbana	75%	150%	10,125
A.22 Manipulación de programas	2	3	6	S2 G.Urbana	75%	150%	6,75
A.11 Acceso no autorizado	2	3	6	S2 G.Urbana	75%	150%	6,75
Gestión geoportal							
E.1 Errores de los usuarios	3	3	9	S2 G.Urbana	50%	150%	6,75
A.22 Manipulación de programas	2	3	6	S2 G.Urbana	50%	150%	4,5
A.11 Acceso no autorizado	2	3	6	S2 G.Urbana	50%	150%	4,5
Gestión cementerio							
A.11 Acceso no autorizado	1	3	3	S2 G.Urbana	25%	150%	1,125
A.15 Manipulación deliberada de la información	1	5	5	S2 G.Urbana	25%	150%	1,875
Gestión cultura, deportes, juventud y participación							
E.1 Errores de los usuarios	3	2	6	S2 G.Urbana	25%	150%	2,25
A.5 Suplantación del usuario	2	3	6	S2 G.Urbana	25%	150%	2,25

A.7 Uso no previsto	2	3	6	S2 G.Urbana	25%	150%	2,25
APP móvil							
A.15 Manipulación deliberada de la información	2	4	8	S3 Bienestar	20%	125%	2
A.22 Manipulación de programas	2	4	8	S3 Bienestar	20%	125%	2
A.24 Denegación de servicio	2	3	6	S3 Bienestar	20%	125%	1,5
Gestión espacios públicos							
E.1 Errores de los usuarios	3	2	6	S3 Bienestar	25%	125%	1,875
A.5 Suplantación del usuario	2	3	6	S3 Bienestar	25%	125%	1,875
A.7 Uso no previsto	2	3	6	S3 Bienestar	25%	125%	1,875
Redes sociales							
A.5 Suplantación del usuario	2	3	6	S3 Bienestar	20%	125%	1,5
A.15 Manipulación deliberada de la información	2	4	8	S3 Bienestar	20%	125%	2
Gestión servicios sociales							
A.3 Manipulación de los logs	1	4	4	S4 S.Sociales	100%	150%	6
A.5 Suplantación del usuario	2	5	10	S4 S.Sociales	100%	150%	15
A.6 Abuso de privilegios de acceso	2	5	10	S4 S.Sociales	100%	150%	15
A.11 Acceso no autorizado	2	5	10	S4 S.Sociales	100%	150%	15
A.15 Manipulación deliberada de la información	2	5	10	S4 S.Sociales	100%	150%	15
A.19 Divulgación de información	2	5	10	S4 S.Sociales	100%	150%	15
Servidor de directorio activo							
I.1 Fuego	1	4	4	Todos	80%	150%	4,8
I.5 Avería de origen físico	2	3	6	Todos	80%	150%	7,2
I.6 Corte del suministro eléctrico	1	3	3	Todos	80%	150%	3,6
I.7 Inadecuada temp/humedad	2	3	6	Todos	80%	150%	7,2
I.8 Fallo en los servicios de comunicaciones	2	3	6	Todos	80%	150%	7,2
Puestos de trabajo							
I.5 Avería de origen físico	3	2	6	Todos	80%	150%	7,2
I.6 Corte del suministro eléctrico	2	2	4	Todos	80%	150%	4,8
I.8 Fallo en los servicios de comunicaciones	2	4	8	Todos	80%	150%	9,6
A.25 Robo	2	3	6	Todos	80%	150%	7,2
Dispositivos móviles corporativos							
I.5 Avería de origen físico	3	2	6	Todos	25%	150%	2,25
A.8 Difusión de software dañino	3	3	9	Todos	25%	150%	3,375

A.19 Divulgación de información	2	3	6	Todos	25%	150%	2,25
A.25 Robo	3	2	6	Todos	25%	150%	2,25
Cabina de discos para copias de seguridad							
I.1 Fuego	1	5	5	Todos	10%	150%	0,75
I.5 Avería de origen físico	2	4	8	Todos	10%	150%	1,2
I.6 Corte del suministro eléctrico	2	3	6	Todos	10%	150%	0,9
I.7 Inadecuada temp/humedad	2	4	8	Todos	10%	150%	1,2
I.8 Fallo en los servicios de comunicaciones	2	3	6	Todos	10%	150%	0,9
I.10 Degradación de los soportes	2	4	8	Todos	10%	150%	1,2
Red LAN interna							
I.1 Fuego	1	4	4	Todos	90%	150%	5,4
I.5 Avería de origen físico	2	4	8	Todos	90%	150%	10,8
I.6 Corte del suministro eléctrico	2	3	6	Todos	90%	150%	8,1
I.7 Inadecuada temp/humedad	2	3	6	Todos	90%	150%	8,1
I.8 Fallo en los servicios de comunicaciones	2	3	6	Todos	90%	150%	8,1
Electrónica de red (routers/switches)							
I.1 Fuego	1	4	4	Todos	90%	150%	5,4
I.5 Avería de origen físico	2	4	8	Todos	90%	150%	10,8
I.6 Corte del suministro eléctrico	2	3	6	Todos	90%	150%	8,1
I.7 Inadecuada temp/humedad	2	3	6	Todos	90%	150%	8,1
I.8 Fallo en los servicios de comunicaciones	2	3	6	Todos	90%	150%	8,1
Telefonía							
I.8 Fallo en los servicios de comunicaciones	2	4	8	Todos	25%	150%	3
A.30 Ingeniería Social	2	3	6	Todos	25%	150%	2,25
Conexiones a red SARA							
I.8 Fallo en los servicios de comunicaciones	2	3	6	S1 y S4	90%	150%	8,1
A.11 Acceso no autorizado	2	3	6	S1 y S4	90%	150%	8,1
Aire acondicionado CPD							
I.5 Avería de origen físico	2	4	8	Todos	90%	150%	10,8
I.6 Corte del suministro eléctrico	2	3	6	Todos	90%	150%	8,1
Discos duros externos							
I.5 Avería de origen físico	3	2	6	Todos	5%	150%	0,45
I.10 Degradación de los soportes	3	2	6	Todos	5%	150%	0,45

A.25 Robo	2	3	6	Todos	5%	150%	0,45
Impresoras							
I.5 Avería de origen físico	3	2	6	Todos	10%	150%	0,9
SAI / Grupo electrógeno							
I.5 Avería de origen físico	2	3	6	Todos	10%	150%	0,9
Empresa mantenimiento HW							
E.2 Errores del administrador	2	3	6	Todos	50%	150%	4,5
E.28 Indisponibilidad del personal	2	3	6	Todos	50%	150%	4,5
Conexión WAN							
I.8 Fallo en los servicios de comunicaciones	2	4	8	Todos	75%	150%	9
A.12 Análisis de tráfico	1	4	4	Todos	75%	150%	4,5
IaaS cloud							
E.2 Errores del administrador	2	4	8	Todos	90%	150%	10,8
E.20 Vulnerabilidades	2	4	8	Todos	90%	150%	10,8
A.4 Manipulación de la configuración	1	4	4	Todos	90%	150%	5,4
A.8 Difusión de software dañino	2	4	8	Todos	90%	150%	10,8
A.11 Acceso no autorizado	2	4	8	Todos	90%	150%	10,8
SaaS cloud							
A.11 Acceso no autorizado	2	4	8	Todos	90%	150%	10,8
A.19 Divulgación de información	1	4	4	Todos	90%	150%	5,4
Empresa desarrollo de aplicaciones							
E.2 Errores del administrador	2	4	8	Todos	50%	150%	6
E.28 Indisponibilidad del personal	1	3	3	Todos	50%	150%	2,25
Empresa soporte a sistemas							
E.2 Errores del administrador	2	4	8	Todos	50%	150%	6
E.28 Indisponibilidad del personal	1	3	3	Todos	50%	150%	2,25
CPD propio							
I.1 Fuego	1	5	5	Todos	90%	150%	6,75
I.6 Corte del suministro eléctrico	1	4	4	Todos	90%	150%	5,4
I.7 Inadecuada temp/humedad	2	4	8	Todos	90%	150%	10,8
A.11 Acceso no autorizado	2	4	8	Todos	90%	150%	10,8
Armario comunicaciones							
I.1 Fuego	1	4	4	Todos	90%	150%	5,4

I.6 Corte del suministro eléctrico	1	3	3	Todos	90%	150%	4,05
A.11 Acceso no autorizado	2	3	6	Todos	90%	150%	8,1
Edificio Ayuntamiento							
I.1 Fuego	1	5	5	Todos	90%	150%	6,75
I.6 Corte del suministro eléctrico	1	4	4	Todos	90%	150%	5,4
A.11 Acceso no autorizado	3	2	6	Todos	90%	150%	8,1
Personal funcionario							
E.1 Errores de los usuarios	3	3	9	Todos	100%	150%	13,5
E.28 Indisponibilidad del personal	3	2	6	Todos	100%	150%	9
A.29 Extorsión	2	5	10	Todos	100%	150%	15
A.30 Ingeniería Social	3	3	9	Todos	100%	150%	13,5
Personal externo							
E.28 Indisponibilidad del personal	2	2	4	Todos	80%	150%	4,8
A.29 Extorsión	2	4	8	Todos	80%	150%	9,6

Tabla 9 Calculo riesgo repercutido

Criterios para calcular la probabilidad:

Nivel	Frecuencia
Muy alto	Acostumbra a suceder una o más veces al mes
Alto	Suele suceder hasta 5 veces al año
Medio	Suele suceder una vez al año
Bajo	Sucede puntualmente
Muy bajo	Altamente improbable

Tabla 10 Criterios de cálculo de la probabilidad

Criterios para calcular el impacto:

IMPACTO	
Muy alto	Incapacidad de prestar el servicio, compromiso irreparable de reputación, recuperación imposible antes de 2 semanas, o daño irreparable a terceros
Alto	Servicio solo funcional excepcionalmente, compromiso importante de reputación, recuperación posible en 1 semana
Medio	Servicio prestable mediante medios alternativos, compromiso leve de reputación, recuperación posible en 1 día
Bajo	Servicio degradado y prestable con pérdida de calidad para usuario, molestias a terceros y recuperación posible en < de 4h.
Muy bajo	Servicio degradado pero prestable sin inconvenientes al usuario, molestias a terceros y recuperación posible en < de 1h.

Tabla 11 Criterios de cálculo del impacto

Una vez identificados los niveles de riesgo a los que están expuestos los sistemas de información de CiudadX, el Responsable del Sistema ha establecido de forma ficticia **los 12,5 puntos como el umbral asumible, por ser la mitad del riesgo potencial (25/2)**.

Mediante el proceso de mejora continua al que obliga el ENS, la meta es bajar progresivamente este umbral hasta quedar por debajo del nivel bajo (10 puntos).

2.4.3 Plan de tratamiento de riesgos

El siguiente paso será definir las acciones a llevar a cabo para cada uno de los riesgos identificados, existiendo 4 opciones:

- **Mitigarlos** o reducirlos, generalmente aplicando salvaguardas que reduzcan la probabilidad o el impacto de materialización.
- **Transferirlos** a un tercero, generalmente mediante la externalización o, por ejemplo, contratando un seguro.
- **Asumirlos**, siempre y cuando se encuentren por debajo del umbral que dictamine el responsable del sistema.
- **Eliminarlos**, eliminando por ejemplo el activo o incluso el propio servicio que depende de cierto activo vulnerable.

Una vez identificados los riesgos que quedan sobre el umbral, deben definirse las formas de tratar cada uno de ellos.

La siguiente tabla los resume, a la vez que menciona las acciones a llevar a cabo, con los niveles de riesgo esperados tras su implantación:

Amenaza	Prob.	Imp.	Riesgo absoluto	Sistemas a los que afecta	Multip por dependencias	Multip por criticidad	Riesgo repercutido	¿Es asumible?	Modo de tratamiento	Acción	Fut. P	Fut. I	Riesgo Residual
Sistemas Operativos Servidores													
E.20 Vulnerabilidades	3	5	15	Todos	100%	150%	22,5	NO	Mitigar	Proc. Gest. Vulns	1	4	6
A.8 Difusión de software dañino	2	5	10	Todos	100%	150%	15	NO	Mitigar	Implantar MicroCLAU-DIA	2	3	9
A.5 Suplantación del usuario	2	5	10	Todos	100%	150%	15	NO	Mitigar	Implantar 2FA	1	5	7,5
Windows + ofimática, correo, antivirus													
A.5 Suplantación del usuario	3	4	12	Todos	100%	150%	18	NO	Mitigar	Implantar 2FA	1	5	7,5
A.11 Acceso no autorizado	2	5	10	Todos	100%	150%	15	NO	Mitigar	Proc. Gest. Vulns	1	4	6
Mantenimiento sistemas: monitorización, backup, etc.													
E.20 Vulnerabilidades	3	4	12	Todos	100%	150%	18	NO	Mitigar	Proc. Gest. Vulns	1	4	6
Apache, PHP y JavaScript (portal web)													
E.20 Vulnerabilidades	3	4	12	Todos	100%	150%	18	NO	Mitigar	Proc. Gest. Vulns	1	4	6
Tomcat y Java (aplicaciones internas)													
E.20 Vulnerabilidades	3	4	12	Todos	100%	150%	18	NO	Mitigar	Proc. Gest. Vulns	1	4	6
Base de datos central													
A.18 Destrucción de la información	2	5	10	Todos	100%	150%	15	NO	Mitigar	Externalizar copias en frio offsite	2	3	9

A.19 Divulgación de información	2	5	10	Todos	100%	150%	15	NO	Mitigar	Ofuscar datos sensibles en BBDD	2	2	6
Gestión servicios sociales														
A.5 Suplantación del usuario	2	5	10	S4 S.Sociales	100%	150%	15	NO	Mitigar	Implantar 2FA	1	5	7,5
A.6 Abuso de privilegios de acceso	2	5	10	S4 S.Sociales	100%	150%	15	NO	Mitigar	Medidas antifraude	1	3	4,5
A.11 Acceso no autorizado	2	5	10	S4 S.Sociales	100%	150%	15	NO	Mitigar	Proc. Gest. Vulns	1	4	6
A.15 Manipulación deliberada de la información	2	5	10	S4 S.Sociales	100%	150%	15	NO	Mitigar	Medidas antifraude	1	3	4,5
A.19 Divulgación de información	2	5	10	S4 S.Sociales	100%	150%	15	NO	Mitigar	Ofuscar datos sensibles en BBDD	2	2	6
Personal funcionario														
E.1 Errores de los usuarios	3	3	9	Todos	100%	150%	13,5	NO	Mitigar	Plan de formación	2	2	6
A.29 Extorsión	2	5	10	Todos	100%	150%	15	NO	Mitigar	Medidas antifraude	1	3	4,5
A.30 Ingeniería Social	3	3	9	Todos	100%	150%	13,5	NO	Mitigar	Plan de formación	2	2	6

Tabla 12 Cálculo del riesgo residual

Dichas acciones, siguen un modelo de gestión de riesgos por el cual se documentan los siguientes aspectos:

- **Acción inmediata**: acción puntual dedicada a reducir inmediatamente el riesgo, pudiendo no ser la solución al problema a largo plazo.
- **Análisis de causa:** motivo real por el que existe el riesgo.
- **Acción correctiva:** acción destinada a evitar que el riesgo vuelva a aparecer.

Esta estructura responde al hecho de que no se tomarían las mismas acciones si por ejemplo existe riesgo de incendio en el CPD, motivado por un cableado deficiente, por carecer de medidas de extinción o por utilizarse para almacenar material inflamable.

Además, a cada acción se le asignará un plazo aproximado de ejecución y un responsable, el cual será el **propietario del riesgo**. Dicho propietario no tiene por qué ser quien va a ejecutar las acciones, sino el responsable de velar porque se lleven a buen término.

PTR1 Procedimiento de gestión de vulnerabilidades

- **Acción inmediata:** actualización masiva y puntual de todo el software desactualizado.
- **Análisis de causa:** el software se actualiza mediante actualizaciones automáticas desatendidas por lo que cuando aparecen cuadros de dialogo o hay versiones con cambios mayores, no se detecta por parte de los administradores.
- **Acción correctiva:** implantar un procedimiento de gestión de vulnerabilidades tanto para servidores como para puestos de trabajo y otros dispositivos. Abarcará acciones preventivas como la instalación periódica de actualizaciones de seguridad o la vigilancia activa de nuevas amenazas, además de acciones correctivas como auditorías de seguridad de los sistemas antes de pasar a producción, así como de los ya desplegados.
- **Propietario del riesgo:** responsable de sistemas
- **Plazo:** 6 meses.

PTR2 Instalación de microCLAUDIA

- **Acción inmediata:** ante el riesgo de que un ataque de ransomware se extienda internamente por la red, se debe instalar la herramienta del CCN microCLAUDIA en los servidores, la cual actúa a modo de vacuna contra los *malware* más extendidos evitando su instalación y propagación.
- **Análisis de causa:** el antivirus corporativo incluye teóricamente estas capacidades, pero también las tenían otros ayuntamientos víctimas de ransomware.
- **Acción correctiva:** no se considera necesaria. Con la acción inmediata es suficiente.
- **Propietario del riesgo:** responsable de sistemas
- **Plazo:** 6 meses

PTR3 Implantar doble factor de autenticación mediante APP móvil

- **Acción inmediata**: forzar un cambio masivo de contraseñas
- **Análisis de causa:** se desconfía de que, debido a algún phishing, *malware* o ataque de ingeniería social, las contraseña hayan sido o puedan ser comprometidas ya que llevan tiempo sin cambiarse
- **Acción correctiva**: implantar un sistema de doble factor de autenticación tanto para usuarios como para servidores y establecer una política de caducidad
- **Propietario del riesgo**: responsable de sistemas
- **Plazo**: 6 meses

PTR4 Ofuscar/anonimizar datos sensibles

- **Acción inmediata**: hacer un estudio para ofuscar o cifrar los datos más sensibles de las bases de datos de las aplicaciones, de modo que ni los administradores ni posibles atacantes que consigas acceso a la base de datos, puedan acceder libremente a la información que contiene.
- **Análisis de causa**: no se había tenido en cuenta en la toma de requisitos de los sistemas que tratan esta información.
- **Acción correctiva**: implantar un sistema de toma de requisitos que incluya las consideraciones de seguridad y protección de la información, de modo que sean los responsables de los datos quienes establezcan los niveles de seguridad requeridos, para que luego se implanten controles acordes. Para las herramientas SaaS, incluir esta toma de requisitos para la contratación de modo que se pueda obligar a cumplir con las medidas del ayuntamiento.
- **Propietario del riesgo**: responsable de seguridad
- **Plazo:** 1 año.

PTR5 Copias de seguridad remotas

- **Acción inmediata:** contratar un servicio remoto de copias de seguridad para asegurar la continuidad de la organización ante un ciberataque que comprometa todo el sistema, o una caída masiva por fallos en los sistemas.
- **Análisis de causa:** no se había contemplado la posibilidad de fallo de las copias locales.
- **Acción correctiva:** hacer una revisión anual del plan de copias, donde además de probar a restaurar sistemas, se evalúe la idoneidad del sistema implantado y posibles mejoras.
- **Propietario del riesgo:** responsable de sistemas
- **Plazo:** 6 meses.

PTR6 Medias antifraude

- **Acción inmediata:** implementar en las aplicaciones medidas antifraude, las cuales incluyan controles aleatorios sobre los expedientes en curso, mecanismos para denunciar comportamientos no profesionales, requerir de varios usuarios para tareas especialmente sensibles, así como detectar anomalías en el uso habitual por parte de usuarios correctamente validados.
- **Análisis de causa (mismos que PTR4)**: no se había tenido en cuenta en la toma de requisitos de los sistemas que tratan esta información.
- **Acción correctiva**: implantar un sistema de toma de requisitos que incluya las consideraciones de seguridad y protección de la información, de modo que sean los responsables de los datos quienes establezcan los niveles de seguridad requeridos, para que luego se implanten controles acordes.
- **Propietario del riesgo**: responsable de seguridad
- **Plazo:** 1 año.

PTR7 Formación

- **Acción inmediata:** dar formación sobre ciberseguridad, que abarque tanto nociones básicas, como uso correcto de los sistemas para evitar fallos humanos.
- **Análisis de causa:** no se había considerado hasta ahora por falta de concienciación al respecto
- **Acción correctiva:** crear un plan de formación que cada año analice las necesidades del personal, la tipología de incidentes, y según dicho análisis, se diseñen formaciones destinadas a mitigar los riesgos identificados.
- **Propietario del riesgo:** responsable de recursos humanos.
- **Plazo:** 6 meses

2.4.4 Aceptación formal de riesgos residuales

Con los datos presentados en el apartado anterior, tanto de las acciones que se van a llevar a cabo, como de los niveles esperados de riesgo resultantes, se debe recoger la aceptación formal de los riesgos residuales (aquellos que quedan una vez aplicadas las salvaguardas planteadas).

Un ejemplo de esta aceptación formal se puede consultar en el Anexo II del presente documento

2.5 Declaración de aplicabilidad

Según el ENS, *"la relación de medidas de seguridad seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad.*

[…]Estas medidas y sus refuerzos se seleccionarán teniendo en cuenta

*a) Los **activos** que constituyen los sistemas de información concernidos.*

*b) La **categoría** del sistema, según lo previsto en el artículo 40 y en el anexo I.*

*c) Las decisiones que se adopten para **gestionar los riesgos** identificados."*

Dado que se han identificado los **activos**, se han **categorizado** los sistemas, y se han adoptado medidas para **gestionar los riesgos**, se dispone de todos los ingredientes para confeccionar la declaración. Para facilitar su confección, el CCN proporciona una plantilla en formato Excel[8], en la cual, tras seleccionar el nivel de seguridad de cada una de las dimensiones, se muestran los controles y refuerzos que son de aplicación.

Cabe recordar, que existe un perfil de cumplimiento específico para ayuntamientos como el de CiudadX, el cual simplifica la aplicación de controles, pero que a fecha de redacción de este proyecto no se encuentra actualizado a la nueva versión del ENS, imposibilitando su uso. En su lugar, se ha optado por aplicar los controles necesarios según la categoría como si el perfil no existiera.

Otro matiz destacable, es que el nuevo ENS permite que "*cuando en un sistema de información existan subsistemas que requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación las medidas de seguridad con los refuerzos correspondientes".* Dada la complejidad y coste que supone para una entidad como el Ayuntamiento de CiudadX implantar las medidas de nivel alto para todos sus sistemas, se ha optado aprovechar esta esta opción marcándose en amarillo en el anexo III, aquellas medidas de seguridad particulares de un sistema y los refuerzos que CiudadX ha considerado implantar de entre las opciones disponibles, y en verde aquellas que ha considerado implantar de forma voluntaria.

2.6 Análisis diferencial

El siguiente paso según la guía 883 de implantación del ENS en entidades locales, consiste en hacer un análisis diferencial del cumplimiento de los controles del anexo II del ENS, el cual se puede documentar en la propia declaración de aplicabilidad, por ser un listado exhaustivo de los controles a implantar.

[8] CCN-CERT (2023). Disponible en https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3827-ccn-cert-bp-14-declaracion-de-aplicacibilidad-ens-anexos/file.html (Consultado el 8 de mayo de 2023)

La plantilla mencionada en el apartado anterior incluye dos columnas dedicadas a medir el grado de implantación y el nivel de madurez de cada control, las cuales, aunque no son propiamente parte de la declaración de aplicabilidad, desde 2010 vienen acompañando a estos documentos en la práctica totalidad de las entregas de empresas consultoras y declaraciones propias, por lo que se han convertido en un elemento habitual que pasamos a explicar:

Nivel de madurez: utiliza el conocido modelo de madurez de CMMI el cual define los siguientes 5 niveles:

- L0 – Incompleto
- L1 – Inicial
- L2 – Repetible pero no formalizado
- L3 – Definido formalmente e implantado
- L4 – Medido y monitorizado
- L5 - Optimizado

Grado de implantación: de forma similar, existe una columna en la que para cada control establecemos el grado de nivel de implantación con la siguiente sencilla clasificación:

- G0 – No implantado
- G1 – Implantado parcialmente
- G2 – Implantado totalmente

Podría parecer que ambas métricas se solapan y que con el CMMI sería suficiente (es mundialmente utilizado), pero es posible tener un procedimiento definido, pero no implantado, el cual sería un L3, pero sin embargo un G0 o G1.

Este segundo indicador es de especial importancia en el ENS, ya que si bien es recomendable saber cómo de maduro está un control, al ser una legislación, realmente solo existen 2 estados válidos, implantado o no, siendo todos los medios tonos por debajo de G2, incumplimientos legales.

Una vez analizado el funcionamiento de la plantilla, se ha utilizado para documentar los niveles de cumplimiento y madurez de los controles del ENS sobre los sistemas ficticios de CiudadX, los cuales se pueden consultar en el anexo III junto a la declaración de aplicabilidad.

2.7 Plan de mejora de la seguridad

Como resultado del análisis diferencial se han definido las siguientes tareas, las cuales son complementarias a las del análisis de riesgos, ya que es posible que sea necesario implantar una medida por, por ejemplo, requisito legal, sin que por ello suponga un riesgo relevante para la seguridad de los sistemas TIC.

- **Acción 1**: **Reporte de incidentes.** definir cómo deben reportar los usuarios y ciudadanos los comportamientos anómalos de los sistemas, introduciendo estos reportes en el procedimiento de gestión de incidentes, así como formar a los usuarios en cómo actuar ante estos casos.

  También se incluirá la obligación de notificar incidentes en las credenciales de usuarios y en las pantallas de bienvenida de los diferentes sistemas (desarrollado en anexo V)

  Controles a los que da cumplimiento: org.3

- **Acción 2: Validación de datos:** implantar un proceso de validación de datos de entrada, salida y datos intermedios para los sistemas de nivel alto y para aquellos que en el análisis de riesgos se ha identificado que pueden ser objetivo de fraude interno. Se verá reforzado por con la instalación de un servidor de recogida y firma de registros de actividad de usuarios y administradores (ver a continuación).

  Controles a los que da cumplimiento: op.pl.2

- **Acción 3: Servidor de logs remoto (desarrollado en anexo IV):** se debe desplegar un servidor para recolectar, almacenar y firmar los registros de actividad de usuario. Esto protegerá los registros de ser alterados, ya sea por personal interno o un ataque malicioso.

  Controles a los que da cumplimiento: op.exp.8 R4 y R5, op.pl.2

- **Acción 4: Política de gestión de accesos (desarrollado en anexo V):** el procedimiento actual no recoge todos los requisitos del ENS, algunos de los cuales a pesar de estar implementados no se encuentran correctamente documentados. Es por ello por lo que se va a redactar un procedimiento completo que recoja las necesidades de la organización en todo lo relacionado con el acceso a activos TI, incluyendo desde la gestión por perfiles hasta la complejidad y caducidad de las contraseñas.

  Controles a los que da cumplimiento: op.acc (todos)

- **Acción 5: Componentes certificados:** hacer un estudio de los componentes de seguridad que deben estar certificados y valorar si solicitar al proveedor actual que certifique sus productos, o cambiar a nuevos productos ya certificados. Se prevé que afecte al menos a elementos de segmentación de red y conectividad como el servidor de VPN, la electrónica de red del perímetro, y herramientas de seguridad como el antivirus y su consola de gestión.

  Controles a los que da cumplimiento: op.pl.5, mp.com.2, mp.com.3

- **Acción 6: Plan de continuidad:** revisar el plan de continuidad para que incluya a los proveedores esenciales como un activo más, tanto en la elaboración del BIA como en las pruebas de continuidad, ya que como se puede observar, están reflejados en el análisis de riesgos de forma genérica.

  Controles a los que da cumplimiento: op.ext.3, op.cont.2

- **Acción 7: Segmentación de redes:** cambiar la segmentación mediante redes VLAN a redes VPN para los sistemas especialmente sensibles de modo que queden correctamente aislados y que el hecho de conectar a uno de estos segmentos especialmente protegidos tenga que ser voluntario por parte del usuario, minimizando la posibilidad de ataques malintencionados o acceso de terceros a través de configuraciones débiles de los equipos de usuario autorizados.

  Controles a los que da cumplimiento: mp.com.4

- **Acción 8: Procedimiento de firma y sellado de tiempo:** se debe redactar el procedimiento que regula los mecanismos para utilizar firma digital y sellos de tiempo. Este documento recogerá también los requisitos que tendrá que cumplir, en cuanto a materia de trazabilidad, el servidor de logs firmados mencionado en la acción 3 para que tengan validez legal.

  Controles a los que da cumplimiento: mp.info.3

3 Resultados y trabajos futuros

El presente apartado analiza los últimos pasos del proceso de adecuación de CiudadX al ENS. Temporalmente se sitúa entre 3 y 6 meses después del apartado anterior para haber dado margen para ejecutar las acciones detectadas.

Llegados a este punto,

Partiendo del estado inicial del sistema de gestión de las TIC preexistente en CiudadX

> …tras seguir los pasos de la guía de adecuación (tanto la genérica ,806, como la específica de entidades locales, 883),
>
> …tras crear, aceptar e implantar los procedimientos y normativas requeridos, algunos de los cuales han sido recogidos en el presente documento,
>
> …tras ejecutar las acciones del Plan de Tratamiento de Riesgos y del Plan de Mejora de la Seguridad de los controles,

CiudadX se encuentra en disposición de abordar una auditoría interna, de la cual posiblemente derivarán nuevas no conformidades que deberán ser abordadas antes de la auditoría de certificación.

En el supuesto de superar esta certificación, una vez publicados los distintivos correspondientes según la guía *"CCN-STIC 809 sobre Declaración, Certificación y Aprobación Provisional de conformidad con el ENS y Distintivos de cumplimiento"* se iniciará el proceso de mejora y vigilancia continua que garantice el mantenimiento y evolución del sistema de gestión implantado.

Para cumplir con este plan, se deberán abordar periódicamente (al menos una vez al año o cuando se produzcan cambios relevantes en los sistemas de información) las siguientes tareas, que deberán ser documentadas y cuyas evidencias han de ser registradas para las siguientes auditorías de seguimiento:

- Revisión anual de alto nivel del sistema de gestión de la seguridad: revisión de la política, objetivos de seguridad, valoración de sistemas, composición del comité de seguridad, etc.
- Revisión anual del análisis de riesgos, la declaración de aplicabilidad y aceptación de las opciones de tratamiento de riesgos.
- Pruebas anuales de continuidad de negocio
- Comprobación anual/semestral del buen funcionamiento de las copias de seguridad y pruebas de restauración
- Revisión anual/semestral de reglas del cortafuegos, acompañadas de pruebas de visibilidad de redes y segmentación.
- Actualizaciones continuas del *firmware*, sistema operativo, *middleware* y aplicaciones de todos los sistemas TI.
- Revisión anual/semestral de cuentas de usuario activas, perfiles de usuario y su asignación y caducidad de contraseñas.
- Análisis anual/semestral de incidentes de seguridad para identificar patrones
- Auditoría interna y de certificación cada 2 años
- Revisión anual del plan de formación y capacitación en ciberseguridad del personal.
- Análisis anual de seguridad de los sistemas según su criticidad, especialmente de servicios expuestos a Internet y servicios especialmente sensibles
- Medición y evaluación mensual de la capacidad de los sistemas, así como volumetría y cálculo de desviaciones significativas.
- Comprobación mensual del estado de los SAI con pruebas de arranque del grupo electrógeno.

4 Conclusiones

Una vez concluida la adecuación del caso ficticio de CiudadX, en el presente apartado se analizan las conclusiones del proyecto, analizando cada uno de los objetivos planteados y sus resultados.

Respecto al **primer objetivo** del proyecto, **analizar y destacar aquellos apartados que sean significativamente diferentes de la versión inicial del ENS,** tras abordar la adecuación, aunque el texto de ambas versiones del ENS ha evolucionado mucho, en la práctica el proceso es muy similar, hallándose las principales diferencias, no en el proceso, sino en el contenido de 5 puntos concretos:

- Cambio en el contenido de documentos concretos, como la política de seguridad o el procedimiento de gestión de incidentes.
- Grandes cambios para organizaciones con infraestructuras críticas o servicios esenciales.
- Grandes cambios en el contenido del anexo II en cuanto a los cambios en los propios controles, la aparición de los perfiles de cumplimiento y la nueva figura de los refuerzos.
- Gran ampliación del alcance, especialmente para el sector privado que presta servicios a las administraciones públicas.
- Introducción de la vigilancia continua

Este cambio en el contenido de los apartados, y no en la estructura general de la gobernanza de la seguridad, facilita el cumplimiento y afecta de forma diferente según la casuística de cada organización:

- Los **organismos públicos que quieran abordar la adecuación desde cero** pueden apoyarse en la documentación existente, incluso en la que no se ha actualizado a la nueva versión, ya que, mientras se conozcan los nuevos requisitos, el resto del proceso es similar.
- Los **organismos públicos que quiera migrar de la versión anterior a la actual**, aparte de la gran actualización de controles y medidas, deberán hacer cambios puntuales e incorporar algunos pocos procesos nuevos a su sistema, haciendo que la transición pueda tener poco impacto.
- Los **proveedores y sector privado** en general que deban cumplir con el ENS encontrarán, más escoyos, ya que, aunque se les ha incluido en el alcance, el texto no se ha transformado lo suficiente como para que perciban que son una nueva pieza del engranaje, sino que se les exige un sistema de gestión como el de las administraciones públicas, pero sin serlo.
- Los **operadores de infraestructuras críticas** que se hayan adecuado a la Ley de Protección de Infraestructuras Críticas son los grandes beneficiados, ya que, aunque les espera un proceso de integración de ambos marcos de trabajo, tienen gran parte del trabajo hecho y se facilita la integración de ambas legislaciones para facilitar su llevanza.

Para el caso concreto del caso de estudio, los resultados del proyecto no hacen más que animarlos a la adecuación, ya que el grueso del proceso se mantiene sin cambios, es posible reutilizar recursos existentes, y el único nuevo escoyo relevante será la aplicación de los nuevos controles.

Antes de analizar el siguiente objetivo, cabe destacar que lo anterior hace referencia al proceso de adecuación, pero una vez conseguida (ya sea adecuación, conformidad o certificación), el nuevo ENS incluye una serie de nuevas tareas a realizar periódicamente dentro del marco de la vigilancia continua. Estas están explicadas en el apartado "Resultados y trabajos futuros", y aplicarían tanto a nuevos sistemas como a los que se deben actualizar, por lo que, aunque la adecuación sea similar, el mantenimiento del sistema de gestión de la seguridad requiere nuevos esfuerzos.

Respecto al **segundo objetivo**, **proveer uno de los primeros documentos de ejemplo para entidades locales siguiendo el nuevo ENS,** se considera que se han conseguido 3 hitos importantes: proporcionado un ejemplo de algunos de los principales documentos que más cambios han sufrido:

- **Plan de adecuación** (la práctica totalidad del proyecto): se ha proporcionado una guía y ejemplo del proceso que debe seguir cualquier organización para la adecuación al ENS. Si bien como ya se ha mencionado el proceso no ha sufrido cambios drásticos, se espera que este proyecto ayude a despejar las dudas de aquellos que ven la adecuación como algo inabordable, o a quienes se excusen en la falta de una guía de adecuación al ENS adaptada a la nueva versión.
- **Política de seguridad:** se ha generado uno de los documentos que en teoría más cambios ha sufrido, aunque para el caso concreto de los ayuntamientos no ha sido tan disruptivo como para otras administraciones. En cualquier caso, el ejemplo propuesto tiene aplicación directa para cualquier ayuntamiento que quiera adecuarse al ENS con su propia política, aunque no debe perderse de vista la opción de que las diputaciones, mancomunidades o agrupaciones de ayuntamientos publiquen políticas comunes que les permitan adherirse a ellas.
- **Declaración de aplicabilidad y análisis diferencial**: es el siguiente documento que más cambios ha sufrido con el nuevo ENS. La utilización de la plantilla en formato Excel proporcionada por el CCN facilita enormemente su confección, aunque deben documentarse los cerca de 100 controles de forma similar a como se ha hecho en este proyecto. Fruto de la experiencia propia trabajando con administraciones públicas, se ha valorado cada control documentado niveles de cumplimiento similares a los reales de los ayuntamientos de estos tamaños, lo que, a pesar de ser una valoración subjetiva, pretende ofrecer pistas a quienes aborden estos proyectos, acerca de los puntos donde más deficiencias suelen encontrarse y que requieren una mayor dedicación de esfuerzos.

De los documentos mencionados con un alto número de cambios con la nueva versión, el referente a la **gestión de incidentes** ha sido el único que no se ha abordado en este proyecto. Esta decisión se ha debido al deseo de priorizar otros documentos más genéricos y menos dependientes de la tecnología y particularidades que tiene cada ayuntamiento, además de que se trata de un servicio generalmente externalizado o gestionado con personal externo de empresas especializadas las cuales aportan su propio *know-how* en esta materia.

En lo referente al tercer objetivo del proyecto, **analizar los principales escollos a la adecuación encontrados que justifiquen los bajos niveles de implantación actuales**, se han detectado las siguientes situaciones:

1. **El proceso es 100% abordable para un ayuntamiento de estas dimensiones,** el cual, debido a su tamaño y atribuciones, seguro que cuenta con un departamento mínimo de TI, una infraestructura lo suficientemente grande como ser relativamente madura (de lo contrario el ayuntamiento no podría prestar sus servicios), y un mínimo sistema de gestión y gobierno de las TIC que facilita la adecuación. Seguramente necesiten apoyo externo y contar con horas de consultoría especializada, pero si han sido capaces de migrar servicios a *cloud* o hacer despliegues de plataformas más allá de lo necesario para cubrir mínimos, son capaces de llevar un proyecto así a buen término.
2. Lo anterior **no es aplicable para ayuntamientos pequeños**, ya que, por la naturaleza de sus servicios y tamaño, los recursos de personal están más limitados.
3. Al hilo de la primera afirmación, sino existe un gran impedimento real, **resulta vital dar un empuje inicial** a estos ayuntamientos para que se planteen la adecuación, ya que una vez den los primeros pasos, la certificación está mucho más cerca de lo que puede parecer. Se trata de una apreciación subjetiva, pero es cierto que, una vez entrado en harina, la ejecución del proyecto ha resultado laboriosa, pero con pocos hitos bloqueantes.
4. Algunas iniciativas para impulsar la certificación están suponiendo **solo una simplificación de la adecuación**, sin abordar los problemas de fondo aquí expuestos. Algunos ejemplos:
    4.1. Los **perfiles de cumplimiento** realmente solo alivian ligeramente la implantación de controles complejos, los cuales no suponen una diferencia definitiva a la hora de decidir sobre si abordar la adecuación o no.
    4.2. El uso del nuevo **µCeENS** solo permite la certificación con un mínimo conjunto de medidas de seguridad. Es una buena aproximación para que las pequeñas entidades den sus primeros pasos, pero no otorgan una certificación real en el ENS y se corre el riesgo de que los esfuerzos terminen en ese primer hito.
    4.3. µCeENS y los perfiles de cumplimiento no resultan comprensibles junto al modelo de valoración de sistemas: por ser un ayuntamiento pequeño, si se dispone de sistemas que tratan información muy sensible ¿deberían de tener menos exigencias en cuanto a ciberseguridad?
5. Ambas versiones del ENS han surgido **sin un procedimiento sancionador en caso de incumplimiento y sin partidas presupuestarias del estado en forma de subvenciones** para la adecuación, por lo que se trata de un proyecto que a los ojos de los mandos ejecutivos de los ayuntamientos solo suponen un gasto. Además, se trata de una inversión que aporta beneficios internos a la organización, pero con poca proyección hacia la ciudadanía y poco explotable políticamente, por lo que quienes han de dotar a TI de presupuesto, ven poco aliciente en abordar el proyecto. Prueba de ello es que las empresas de TI que dan servicios a administraciones públicas y que sí que sacan un beneficio de la certificación, tienen en solo **1 año** de vigencia del nuevo ENS un nivel de implantación que triplica a los organismos públicos que llevan **13 años para adecuarse**[9]:

[9] CCN-CERT (2023) Disponible en https://ens.ccn.cni.es/es/ Consultado el 08/05/2023.

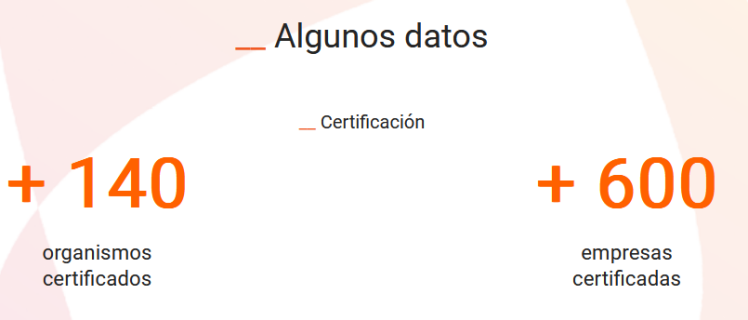


Ilustración 1 Organismos VS empresas certificadas

6. El análisis de riesgos continúa siendo el proceso más costoso y menos "intuitivo o natural" para el personal que aborde la adecuación, suponiendo un escoyo importante que además se aborda en las fases tempranas de la adecuación, posiblemente desmotivando a organizaciones que no tuvieran 100% decidida la implantación. Si bien existen alternativas como PILAR Basic[10], o microPILAR[11], no son aplicables a sistemas de nivel alto como el de un ayuntamiento de este tamaño, a la vez que sus resultados resultan excesivamente vagos. **Es por ello por lo que en este proyecto se ha optado por una implementación de MAGERIT sin el uso de herramientas dedicadas**, el cual es abordable y comprensible por cualquiera con conocimientos ofimáticos, y que al utilizar las fórmulas de cálculo del Libro III, son válidas para cualquier nivel.

[10] PILAR Basic (CCN-CERT, 2023). Disponible en https://pilar.ccn-cert.cni.es/index.php/pilar/pilar-basic . Consultado el 08/05/2023

[11] microPILAR (CCN-CERT, 2023). Disponible en https://pilar.ccn-cert.cni.es/index.php/pilar/pilar-micro . Consultado el 08/05/2023

5 Glosario

Conceptos de MAGERIT

ACTIVO Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

AMENAZA Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización

IMPACTO Consecuencia que sobre un activo tiene la materialización de una amenaza

PROBABILIDAD Tasa de ocurrencia de una amenaza

RIESGO Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización

VULNERABILIDAD Una debilidad que puede ser aprovechada por una amenaza.

Conceptos del ENS

CATEGORÍA DE UN SISTEMA Es un nivel, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios. ENS.

INFORMACIÓN Caso concreto de un cierto tipo de información.

INCIDENTE DE SEGURIDAD Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información. ENS.

MEDIDAS DE SEGURIDAD Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación. ENS.

POLÍTICA DE SEGURIDAD Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

RESPONSABLE DE LA INFORMACIÓN Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

RESPONSABLE DEL SERVICIO Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

RESPONSABLE DEL SISTEMA Persona que se encarga de la explotación del sistema de información.

SERVICIO Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos

SISTEMA DE INFORMACIÓN Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

6 Bibliografía

6.1 Legislación

- Esquema Nacional de Seguridad, (**versión actual 2022)**, Boletín Oficial del Estado (BOE) Disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-2022-7191 (Consultada el 1 de abril de 2023)
- Esquema Nacional de Seguridad (**versión inicial 2007**) Boletín Oficial del Estado (BOE) Disponible en https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330 (Consultada el 1 de abril de 2023)
- Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos. Boletín Oficial del Estado (BOE) Disponible en https://www.boe.es/buscar/act.php?id=BOE-A-2007-12352 (Consultada el 1 de abril de 2023)
- Ley de Protección de Infraestructuras Críticas, Boletín Oficial del Estado (BOE 2023) - Disponible en https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf. (Consultado el 08/05/2023)
- Ley 7/1985 Reguladora de las Bases del Régimen Local (LBRL) Boletín Oficial del Estado (BOE) (1985) Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1985-5392 (Consultada el 5 de abril de 2023)

6.2 Guías CCN STIC y otra documentación CCN

- [TODAS] Centro Criptológico Nacional (CCN) (2023) Disponible en https://www.ccn-cert.cni.es/ (Consultadas el 1 de abril de 2033)
- CCN-STIC 800, Glosario de términos y abreviaturas (2016) Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/499-ccn-stic-800-glosario-de-terminos-y-abreviaturas-del-ens/file.html
- CCN-STIC-801 Responsabilidades y Funciones en el ENS (2019) Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html
- CCN-STIC-802 Auditoría del ENS (2017) Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/502-ccn-stic-802-auditoria-del-ens/file.html
- CCN-STIC-803 Valoración de Sistemas en el ENS (2020), Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html
- CCN-STIC-804 ENS. Guía de implantación (2017), Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file.html
- CCN-STIC-805 Política de Seguridad de la Información (2023) Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/508-ccn-stic-805-politica-de-seguridad-de-la-informacion/file.html
- CCN-STIC-806 Plan de Adecuación al ENS (2020) Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/511-ccn-stic-806-plan-de-adecuacion-al-ens/file.html
- CCN-STIC-808 Verificación del cumplimiento de las medidas en el ENS (2022), Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-

nacional-de-seguridad/518-ccn-stic-808-verificacion-del-cumplimiento-de-las-medidas-en-el-ens/file.html

- CCN-STIC-809 Declaración, Certificación y Aprobación Provisional de conformidad con el ENS y Distintivos de cumplimiento (2022), Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/1279-ccn-stic-809-declaracion-de-conformidad-con-el-ens/file.html
- CCN-STIC 883 Guía de Implantación del ENS para EELL (2020), Disponible en https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/3758-ccn-stic-883-guia-de-implantacion-del-ens-para-entidades-locales/file.html
- CCN-STIC 883C Perfil de Cumplimiento Específico 20.000>Ayuntamientos <75.000 (2020), Disponible en https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/4994-ccn-stic-883c-perfil-cumplimiento-especifico-ayuntamientos-20-000.html
- CCN-STIC 883 Anexo II. Plan de Adecuación al ENS 20.000>Ayuntamientos <75.000 (2020), Disponible en https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/4991-ccn-stic-883-anexo-ii-plan-adecuacion-ayuntamientos-20-000/file.html
- CCN-CERT BP 14 Declaración de Aplicabilidad ENS - Plantilla declaración (2023), Disponible en https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3827-ccn-cert-bp-14-declaracion-de-aplicacibilidad-ens-anexos/file.html
- CCN-STIC-610A22 Guía de aplicación de perfilado de seguridad para Red Hat Enterprise Llinux (2022) Disponible en: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6768-ccn-stic-610a22-perfilado-de-seguridad-red-hat-enterprise-linux-9-0/file.html
- Herramienta MicroCLAUDIA, Disponible en https://www.ccn-cert.cni.es/soluciones-seguridad/microclaudia.html
- Herramienta μCeENS, Disponible en https://ens.ccn.cni.es/es/conformidad/microceens

6.3 Otras fuentes consultadas

- Objetivos de desarrollo sostenible de Naciones Unidas (UN) (2023) Disponible en: https://www.un.org/sustainabledevelopment/es/peace-justice/ (Consultada el 1 de abril de 2023)
- MAGERIT versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I (método) y Libro II (catálogo de elementos), Gobierno de España (2023) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html (Consultada el 11 de abril de 2023)
- Configurar sistema de logs remotos en Red Hat, Red Hat (2023) Disponible en: https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/8/html/configuring_basic_system_settings/configuring-a-remote-logging-solution_configuring-basic-system-settings#the-rsyslog-logging-service_configuring-a-remote-logging-solution (Consultada el 12 de junio de 2023)
- Cifrado TLS en rsyslog, Rsyslog (2008), Disponible en https://www.rsyslog.com/doc/v8-stable/tutorials/tls_cert_summary.html Consultado el 12 de junio de 2023
- Administración de servidores, Remo Suppi Boldrito. UOC (2023) Disponible en https://openaccess.uoc.edu/bitstream/10609/61265/2/Administraci%C3%B3n%20avanzada%20del%20sistema%20operativo%20GNU_Linux_M%C3%B3dulo2_Administraci%C3%B3n%20de%20servidores.pdf . Consultado el 12 de junio de 2023
- Modelo CMMI. ISACA (2023). Disponible en https://cmmiinstitute.com/ (Consultado el 6 de junio de 2023)
- Modelo RBAC Cloudflare (2023). Disponible en https://www.cloudflare.com/es-es/learning/access-management/role-based-access-control-rbac/ . Consultado el 13 de junio de 2023

7 Anexos

7.1 Anexo I Política de Seguridad

El Ayuntamiento de CiudadX, consciente de la importancia de la seguridad de la información que trata y de los servicios que presta, publica la siguiente política en la que se compromete administrar sus sistemas TIC (Tecnologías de Información y Comunicaciones), con diligencia y tomando las medidas adecuadas para protegerlos frente a cualquier daño pueda afectar a su disponibilidad, integridad o confidencialidad.

Para ello tomará las medidas preventivas oportunas, supervisará la actividad de los sistemas continuamente y reaccionará con presteza ante los incidentes que puedan materializarse.

Objetivos y misión

El Ayuntamiento de CiudadX tiene según la Constitución Española, la misión de gobernar y administrar la ciudad.

Con el fin de hacerlo con objetividad, velando por los intereses generales y actuando eficazmente, se ha propuesto los siguientes objetivos:

- Dotar a la ciudadanía de calidad de vida mediante la provisión de servicios sociales adecuados, opciones de ocio y cultura enriquecedoras, y fomentando iniciativas saludables y que mejoren el medio ambiente local.
- Mantener y hacer evolucionar de forma sostenible las infraestructuras municipales, haciendo un uso responsable de las mismas, y velando por su disfrute por parte de los intereses populares.
- Velar por el desarrollo económico de la ciudad mediante inversiones en sectores estratégicos, fomentando el comercio local, y proveyendo de herramientas y formación a la ciudadanía para que pueda desarrollar y mejorar sus actividades económicas.
- Proveer una administración eficaz, cercana, y accesible para todos los ciudadanos, fomentando el uso de la tecnología, y acercando la administración y el gobierno al pueblo.

Marco regulatorio

El marco regulatorio relacionado con la protección de la información y los servicios de CiudadX, así como del cumplimiento de la legislación vigente en materia TIC, es el siguiente:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Instrucciones Técnicas de Seguridad del Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

ORGANIZACIÓN DE LA SEGURIDAD

La organización de la Seguridad de la Información ha establecido los siguientes roles y responsabilidades, cuyas designaciones personales pueden consultarse en las actas de los plenos municipales:

- Delegado de Protección de Datos (DPD): debe asesorar a los responsables y encargados del tratamiento en materia de protección de datos y supervisar el cumplimiento del RGPD y la LOPDGDD en el ayuntamiento.
- Responsables de Información: debe establecer los niveles de seguridad que se deben aplicar a la información y asumir los riesgos residuales asociados a la información en el análisis de riesgos.
- Responsables de los Servicios: debe establecer los niveles de seguridad que se deben aplicar a los servicios que tratan la información y asumir los riesgos residuales asociados a la información en el análisis de riesgos.
- Responsable de Seguridad: define las medidas de seguridad que deben aplicarse a los sistemas para cumplir con los requisitos establecidos por los responsables de la información y los servicios, además de velar por la seguridad general de la plataforma TIC, y proporcionar asesoramiento en dicha materia al resto de departamentos.
- Responsable del Sistema: es el encargado de aplicar las medidas de seguridad identificadas por el Responsable de Seguridad y velar por su cumplimiento.
- Comité de Seguridad de la Información: comité formado por las figuras anteriores y el alcalde y secretario municipal. El comité es el encargado de debatir decisiones estratégicas que puedan influir en la seguridad de los sistemas y cuyas decisiones sean transversales a las diferentes figuras de sus miembros y que por tanto requieran de consenso. También podrá ser convocado ante incidentes críticos y para la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

La elección y designación de estos roles se hará por votación en pleno municipal ordinario y tendrán una vigencia de 2 años renovables.

Documentación

A la presente política le complementan otras normativas, procedimientos e instrucciones técnicas de carácter confidencial que contribuyen a la protección de los sistemas municipales y al cumplimiento legal y normativo.

Estos incluyen entre otros, los siguientes documentos:

- Normativa de gestión de accesos
- Normativa de seguridad física
- Normativa de mejora continua.
- Normativa de uso seguro de sistemas TIC
- Normativa de protección de la información y los datos personales
- Procedimiento de análisis y gestión de riesgos TIC.
- Procedimiento de gestión del personal y formación
- Procedimiento de gestión y mantenimiento de sistemas y continuidad de negocio.
- Procedimiento de gestión de incidentes.
- Instrucción técnica para la contratación de sistemas TIC.
- Instrucción técnica para la verificación de seguridad de los sistemas.

DATOS DE CARÁCTER PERSONAL

El Ayuntamiento de CiudadX cumple con las diferentes normativas de protección de datos personales, cuyos detalles están recogidos en el correspondiente documento de seguridad y su Registro de actividades de tratamiento se encuentra publicado en su página web.

Adicionalmente, como parte de esta política, se desea poner de manifiesto que solo se recogerán datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

7.2 Anexo II Aceptación formal de riesgos residuales

En CiudadX, a 09 de mayo de 2023

De acuerdo con los resultados obtenidos en el Análisis de Riesgos realizado en fecha abril de 2023, el Ayuntamiento de CiudadX toma las siguientes decisiones acerca de los riesgos detectados:

1. Mediante las acciones del plan de tratamiento de riesgos, se reducirán los niveles de riesgo detectados hasta que estos sean menores al máximo asumible respetando el equilibrio entre el nivel de seguridad alcanzado y el coste de implantación de salvaguardas.
2. En caso de que durante la ejecución de las acciones se detecte la imposibilidad de llevarlas a cabo, se ejecutarán otras similares que consigan reducir los riesgos, al menos a los niveles comprometidos.
3. Se asumirán los riesgos cuyo valor quede por debajo de los niveles aceptables establecidos para 2023.

Firmado:

El alcalde de CiudadX

7.3 Anexo III Declaración de aplicabilidad e insuficiencias

Código	Descripción	Nivel Madurez	Grado Implem.	Cat. Sistema	Aplicabilidad	Cómo aplica	Acción
org	**Marco organizativo**						
org.1	Política de seguridad	L3	G2	ALTA	aplica	Se dispone de una política de seguridad que cumple con los requisitos del ENS publicada en la web municipal	
org.2	Normativa de seguridad	L3	G2	ALTA	aplica	Se dispone de la totalidad de los documentos requeridos en el gestor documental	
org.3	Procedimientos de seguridad	L2	G1	ALTA	aplica	No se dispone de la totalidad de los documentos requeridos. Falta org.3.3: Cómo identificar y reportar comportamientos anómalos	Se redactará el documento que falta
org.4	Proceso de autorización	L3	G2	ALTA	aplica	Se dispone de la totalidad de los documentos requeridos en el gestor documental	
op	**Marco operacional**						
op.pl	***Planificación***						
op.pl.1	Análisis de riesgos	L4	G2	ALTA	+R2	Se dispone de un análisis de riesgos formal que cumple los requisitos del ENS, así como de un plan de tratamiento de riesgos	
op.pl.2	Arquitectura de Seguridad	L2	G1	ALTA	+R1 +R2 +R3	Falta formalizar algunos aspectos del control, como el R3 de validación de datos de entrada/salida/intermedios, que solo se aplicará a los sistemas de nivel alto.	Se implantará el proceso
op.pl.3	Adquisición de nuevos componentes	L3	G2	ALTA	aplica	Existe el proceso formal de adquisición de componentes el cual contempla los requisitos de seguridad. Contemplado en el procedimiento "Gestión de cambios TIC"	
op.pl.4	Dimensionamiento/gestión de la capacidad	L3	G2	ALTA	+R1	La gestión de la capacidad está incluida en la gestión de cambios y se incluye en la mejora continua. Documentado en "Gestión de cambios TIC"	

op.pl.5	Componentes certificados	L2	G1	ALTA	Aplica +R2	Algunos de los componentes de seguridad no están certificados por haberse contratado antes de la adecuación al ENS. Los que lo están se pueden consultar en los detalles del OCS Inventory. En dicho OCS se encuentran las características que dan cumplimiento a R2.	Se trasladará a los fabricantes para valorar cambiar de proveedor
op.acc	***Control de acceso***						
op.acc.1	Identificación	L1	G1	ALTA	+R1	Se cumple parcialmente con los requisitos del control. Documentado en "Política de gestión de accesos"	Se necesita hacer un estudio profundo de los detalles del control para ultimar algunas configuraciones
op.acc.2	Requisitos de acceso	L3	G2	ALTA	+R1 +R2	Existen perfiles de acceso según las necesidades, los recursos están protegidos mediante autenticación y en general se cumple con los requisitos del control. Documentado en "Política de gestión de accesos"	Existe un NAC[12] para dar cumplimiento voluntario a R2.
op.acc.3	Segregación de funciones y tareas	L3	G2	ALTA	+R1	Existe una correcta segregación de funciones que contempla los requisitos del ENS. Documentado en "Política de gestión de accesos"	
op.acc.4	Proceso de gestión de derechos de acceso	L3	G2	ALTA	aplica	Se cumple con el principio del mínimo privilegio y el "need to know", cumpliendo con la totalidad del control. Documentado en "Política de gestión de accesos"	
op.acc.5	Mecanismo de autenticación (usuarios externos)	L2	G1	ALTA	+ [R2 o R3	Se cumple con la mayoría de los requisitos, aunque faltan puntos por documentar en "Política de gestión de accesos" y el 2FA (refuerzo 2) ya mencionado en el análisis de riesgos. Adicionalmente las cuentas se desactivan por inactividad para dar cumplimiento voluntario a R7.	Completar la "Política de gestión de accesos"

[12] ¿Qué es un NAC? CISCO, Disponible en https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html, Consultado el 13 de junio de 2023

op.acc.6	Mecanismo de autenticación (usuarios de la organización)	L2	G1	ALTA	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9	Se cumple con la mayoría de los requisitos, aunque faltan puntos por documentar en "Política de gestión de accesos" y el 2FA (refuerzo 2) ya mencionado en el análisis de riesgos.	Completar la "Política de gestión de accesos"
op.exp	***Explotación***						
op.exp.1	Inventario de activos	L4	G2	ALTA	Aplica +R2 + R4	Existe una aplicación de inventario (OCS Inventory) centralizada con todos los componentes. Además, se dispone de un software de monitorización de servidores y equipos para dar cumplimiento voluntario a R2 y R4	
op.exp.2	Configuración de seguridad	L3	G2	ALTA	aplica	Los equipos se plataforman de forma segura antes de su puesta en marcha cumpliendo con los requisitos del control. Existe una instrucción técnica "Plataformado de equipos", que sigue las guías del CCN	
op.exp.3	Gestión de la configuración de seguridad	L2	G1	ALTA	+R1 +R2 +R3	La gestión de la configuración es correcta (documentado en "Gestión de cambios TIC") pero falta hacer una gestión adecuada de las vulnerabilidades de los sistemas	Ya identificado en el plan de tratamiento de riesgos
op.exp.4	Mantenimiento y actualizaciones de seguridad	L2	G1	ALTA	+R1 +R2	Falta mejorar la forma en que se gestionan las actualizaciones y la corrección de vulnerabilidades	Ya identificado en el plan de tratamiento de riesgos
op.exp.5	Gestión de cambios	L4	G2	ALTA	+R1	Existe un procedimiento robusto de gestión de cambios con un alto nivel de madurez llamado "Gestión de cambios TIC", aunque las pruebas de R1.1 solo se realizan de forma exhaustiva para los sistemas de nivel alto.	
op.exp.6	Protección frente a código dañino	L3	G2	ALTA	+R1 +R2 +R3 +R4	Se dispone de antivirus en todo el parque de dispositivos del ayuntamiento y se gestiona adecuadamente	
op.exp.7	Gestión de incidentes	L3	G2	ALTA	+R1 +R2 +R3	Se dispone de un procedimiento adecuado llamado "Gestión de incidentes de seguridad"	
op.exp.8	Registro de la actividad	L3	G2	ALTA	+R1 +R2 +R3 +R4 +R5	Todos los sistemas generan los registros que sus responsables han considerado, pero se almacenan en local, con el riesgo de que se comprometan.	Crear un servidor central de registros para su salvaguarda, en consonancia con las herramientas antifraude del análisis de riesgos para el refuerzo 5

op.exp.9	Registro de la gestión de incidentes	L3	G2	ALTA	aplica	La gestión de incidentes se realiza mediante soluciones proporcionadas por el CCN-CERT	
op.exp.10	Protección de claves criptográficas	L3	G2	ALTA	+R1	Se realiza una gestión adecuada de las claves criptográficas y certificados según el ENS	
op.ext	***Recursos externos***						
op.ext.1	Contratación y acuerdos de nivel de servicio	L3	G2	ALTA	aplica	Las condiciones están contempladas tanto en las cláusulas contractuales, como en los pliegos públicos.	
op.ext.2	Gestión diaria	L0	G0	ALTA	aplica	Existe un sistema de monitorización que controla el uso de los sistemas y las necesidades de mantenimiento	
op.ext.3	Protección de la cadena de suministro	L2	G1	ALTA	aplica	En el análisis de riesgos se contemplan parcialmente los impactos asociados a la cadena de suministro, pero no es exhaustivo ni el plan de continuidad contempla a los proveedores	Se debe revisar el plan de continuidad para que contemple a los proveedores
op.ext.4	Interconexión de sistemas	L3	G2	ALTA	+R1	Requisito cubierto por la documentación y proceso de conexión con la red SARA	
op.nub	***Servicios en la nube***						
op.nub.1	Protección de servicios en la nube	L3	G2	ALTA	+R1 +R2	Los proveedores de servicios cloud están certificados en el ENS para nivel ALTO	
op.cont	***Continuidad del servicio***						
op.cont.1	Análisis de impacto	L3	G2	ALTA	aplica	Como paso previo al análisis de riesgos se realiza un análisis de impacto	
op.cont.2	Plan de continuidad	L3	G1	ALTA	Aplica +R1	El plan de continuidad del ayuntamiento (que da cumplimiento voluntario a R1) contempla la continuidad de los servicios de ciberseguridad, aunque se deben matizar los puntos de la cadena de suministro relacionados con el control op.ext.3	Ya contemplado en op.ext.3
op.cont.3	Pruebas periódicas	L3	G2	ALTA	aplica	Se realizan pruebas periódicas del plan de continuidad	
op.cont.4	Medios alternativos	L3	G2	ALTA	aplica	El plan de continuidad contempla los medios alternativos necesarios para la prestación del servicio	
op.mon	***Monitorización del sistema***						

op.mon.1	Detección de intrusión	L3	G2	ALTA	+R1 +R2	Se dispone de un detector de intrusos en el perímetro de la red, además de agentes (Wazuh) en los servidores a modo de HostIDS	
op.mon.2	Sistema de métricas	L3	G2	ALTA	+R1 +R2	Constantemente se recogen las métricas necesarias para medir el estado de la seguridad, y se revisan mensualmente en busca de desviaciones de los umbrales establecidos	
op.mon.3	Vigilancia	L3	G2	ALTA	+R1 +R2 +R3 +R4 +R5 +R6	Control cubierto por las herramientas del CCN desplegadas en el ayuntamiento junto al gestor de incidencias, aunque debido a la complejidad del análisis de estos datos, solo se monitorizan los sistemas de nivel alto.	
mp	**Medidas de protección**						
mp.if	***Protección de las instalaciones e infraestructuras***						
mp.if.1	Áreas separadas y con control de acceso	L3	G2	ALTA	aplica	El CPD propio dispone de control de acceso	
mp.if.2	Identificación de las personas	L3	G2	ALTA	aplica	El CPD propio dispone de control de acceso	
mp.if.3	Acondicionamiento de los locales	L3	G2	ALTA	aplica	El CPD propio dispone de control de temperatura y humedad, cableado ordenado y prevención de desastres industriales	
mp.if.4	Energía eléctrica	L3	G2	ALTA	+R1	El CPD propio dispone de control de temperatura y humedad, cableado ordenado y prevención de desastres industriales	
mp.if.5	Protección frente a incendios	L3	G2	ALTA	aplica	El CPD propio dispone de control de temperatura y humedad, cableado ordenado y prevención de desastres industriales	
mp.if.6	Protección frente a inundaciones	L3	G2	ALTA	aplica	El CPD propio dispone de control de temperatura y humedad, cableado ordenado y prevención de desastres industriales	
mp.if.7	Registro de entrada y salida de equipamiento	L3	G2	ALTA	aplica	Según el procedimiento de Gestión de cambios TIC, cuando un elemento es desplazado, se registra tanto en la herramienta de ticketing como en el inventario.	
mp.per	***Gestión del personal***						
mp.per.1	Caracterización del puesto de trabajo	L3	G2	ALTA	aplica	En el documento "Seguridad de los RRHH" se documentan los perfiles de usuarios, sus requisitos, y el resto de información solicitada en el control.	

mp.per.2	Deberes y obligaciones	L3	G2	ALTA	+R1	En el documento "Seguridad de los RRHH" se documentan los perfiles de usuarios, sus requisitos, y el resto de información solicitada en el control.	
mp.per.3	Concienciación	L1	G1	ALTA	aplica	Aunque existen acciones formativas sobre seguridad y concienciación, no forman parte de un plan organizado	Ya contemplado en el análisis de riesgos (PTR7).
mp.per.4	Formación	L1	G1	ALTA	aplica	Aunque existen acciones formativas sobre seguridad y concienciación, no forman parte de un plan organizado	Ya contemplado en el análisis de riesgos (PTR7).
mp.eq	***Protección de los equipos***						
mp.eq.1	Puesto de trabajo despejado	L3	G2	ALTA	+R1	En el documento "medidas básicas de seguridad" se incluyen referencias al puesto de trabajo despejado	
mp.eq.2	Bloqueo de puesto de trabajo	L3	G2	ALTA	+R1	Los puestos de trabajo se bloquean automáticamente, llegándose a cerrar las sesiones en caso de ausencia prolongada para los sistemas con autenticación de nivel alto (R1)	
mp.eq.3	Protección de dispositivos portátiles	L3	G2	ALTA	+R1 +R2	La gestión segura de los equipos está cubierta mediante el cifrado de los mismos, el registro de cambios (Gestión de cambios TIC), y el procedimiento de gestión de incidentes de seguridad, entre otros.	
mp.eq.4	Otros dispositivos conectados a la red	L3	G2	ALTA	+R1 + R2	Se realiza un inventariado automático de dispositivos que evita la conexión de equipos no autorizados, existiendo para ellos una red independiente de cortesía. La conexión de dispositivos autorizados se gestiona mediante la gestión de cambios habitual. Respecto a R1, productos certificados, se encuentra documentado en op.pl.5 Adicionalmente, existe un NAC que da cumplimiento voluntario al refuerzo R2.	
mp.com	***Protección de las comunicaciones***						
mp.com.1	Perímetro seguro	L3	G2	ALTA	aplica	Se dispone de 2 firewalls en cascada de diferentes fabricantes que separan la red interna de la DMZ e Internet	

mp.com.2	Protección de la confidencialidad	L3	G1	ALTA	+R1 +R2 +R3	Existe una VPN corporativa para conexiones remotas, aunque no está certificada por el CCN. El resto de las conexiones con sitios que requieren confianza se realiza mediante SSL estableciendo conexiones punto a punto	Considerar migrar a una solución certificada, en la línea de la acción del control op.pl.5
mp.com.3	Protección de la integridad y de la autenticidad	L3	G1	ALTA	+R1 +R2 +R3 +R4	Existe una VPN corporativa para conexiones remotas, aunque no está certificada por el CCN. El resto de conexiones con sitios que requieren confianza se realiza mediante SSL estableciendo conexiones punto a punto	Considerar migrar a una solución certificada, en la línea de la acción del control op.pl.5
mp.com.4	Separación de flujos de información en la red	L3	G2	ALTA	+[R2 o R3] +R4	La red del ayuntamiento está segmentada según su uso: servidores de aplicaciones internas, DMZ, usuarios, informática, invitados, externos y red protegida (alcaldía)	La configuración actual es mediante el uso de redes VLAN de modo que se separarán los servidores sensibles que hacen que el sistema sea de nivel alto y se limitará su acceso mediante VPN (refuerzo3).
mp.si	***Protección de los soportes de información***						
mp.si.1	Marcado de soportes	L3	G2	ALTA	aplica	Los soportes se etiquetan y gestionan de forma segura según lo documentado en "medidas básicas de seguridad"	
mp.si.2	Criptografía	L3	G2	ALTA	+R1 +R2	Los soportes se etiquetan y gestionan de forma segura según lo documentado en "medidas básicas de seguridad", lo cual incluye el cifrado de R1. Para el cifrado de copias de R2, se aplica únicamente a los datos de nivel alto.	
mp.si.3	Custodia	L3	G2	ALTA	aplica	Los soportes se etiquetan y gestionan de forma segura según lo documentado en "medidas básicas de seguridad". Adicionalmente, los usuarios aceptan las condiciones de uso seguro de los sistemas al ser dados de alta	
mp.si.4	Transporte	L3	G2	ALTA	aplica	Los soportes se etiquetan y gestionan de forma segura según lo documentado en "medidas básicas de seguridad"	

mp.si.5	Borrado y destrucción	L3	G2	ALTA	+R1	Los soportes se etiquetan y gestionan de forma segura según lo documentado en "medidas básicas de seguridad"	
mp.sw	***Protección de las aplicaciones informáticas***						
mp.sw.1	Desarrollo de aplicaciones	L3	G2	ALTA	+R1 +R2 +R3 +R4	En el procedimiento de "desarrollo y despliegue seguro de aplicaciones" se documentan los 3 entornos (Desa, pre y pro), así como la metodología, aceptación y custodia de los datos de prueba entre otros	
mp.sw.2	Aceptación y puesta en servicio	L3	G2	ALTA	+R1	En el procedimiento de "desarrollo y despliegue seguro de aplicaciones" se documentan los 3 entornos (Desa, pre y pro), así como la metodología, aceptación y custodia de los datos de prueba entre otros	
mp.info	***Protección de la información***						
mp.info.1	Datos personales	L3	G2	ALTA	aplica	El ayuntamiento hizo la adecuación a la nueva ley de protección de datos y al reglamento europeo, superando una auditoría externa de forma satisfactoria	
mp.info.2	Calificación de la información	L3	G2	ALTA	aplica	El documento "protección de la información", de obligado cumplimiento, recoge los requisitos y medidas de seguridad a aplicar a la información que dan cumplimiento al presente control	
mp.info.3	Firma electrónica	L2	G1	ALTA	+R1 +R2 +R3 +R4	A pesar de que los trabajadores conocen las restricciones a la hora de trabajar con firma electrónica, no se dispone de una política formal. El requerimiento de firma electrónica avanzada con doble factor se reserva solo a los sistemas de nivel alto para dar cumplimiento a R4	Crear el procedimiento de firma digital y sello de tiempo del ayuntamiento
mp.info.4	Sellos de tiempo	L2	G1	ALTA	aplica	A pesar de que los trabajadores conocen las restricciones a la hora de trabajar con sellos de tiempo, no se dispone de una política formal	Crear el documento de firma digital y sello de tiempo del ayuntamiento
mp.info.5	Limpieza de documentos	L3	G2	ALTA	aplica	El documento "protección de la información", de obligado cumplimiento, recoge los requisitos y medidas de seguridad a aplicar a la información que dan cumplimiento al presente control	

mp.info.6	Copias de seguridad	L2	G1	ALTA	+R1 +R2	Existe una instrucción técnica con información acerca de cómo realizar y proteger las copias de seguridad. No obstante, no se realizan copias de seguridad en ubicaciones alternativas.	Ya abordado en el análisis de riesgos (PTR5)
mp.s	***Protección de los servicios***						
mp.s.1	Protección del correo electrónico	L3	G2	ALTA	aplica	Se utilizan las herramientas de seguridad para la protección del correo y su contenido provistas por el proveedor. Las normas de cómo usarlas están documentadas en "medidas básicas de seguridad".	
mp.s.2	Protección de servicios y aplicaciones web	L3	G2	ALTA	+R2 +R3	Durante el desarrollo de los sitios web, atendiendo al documento de "desarrollo y despliegue seguro de aplicaciones", se securizan las mismas antes de su despliegue, el cual se hace de forma segura mediante la gestión de cambios, y se vela por su mantenimiento mediante la gestión de vulnerabilidades	
mp.s.3	Protección de la navegación web	L3	G2	ALTA	+R1	La navegación se hace mediante un proxy intermedio que implementa los requisitos de seguridad establecidos por el ENS	
mp.s.4	Protección frente a denegación de servicio	L3	G2	ALTA	+R1	Se dispone de un servicio anti-DDoS contratado con el proveedor de comunicaciones	

Tabla 13 Declaración de aplicabilidad

Marcado en amarillo, los refuerzos seleccionados según la valoración del sistema

Marcados en verde, los refuerzos seleccionados voluntariamente

7.4 Anexo IV Instalación de un servidor de logs centralizado

Nota: el presente documento da cumplimiento a los controles op.exp.8 y op.pl.2.

A continuación, se detalla el procedimiento para crear un servidor centralizado de logs con el fin de almacenarlos y firmarlos digitalmente a modo de evidencia ante investigaciones sobre trazabilidad de accesos.

Esta instalación está motivada por los siguientes puntos clave:

- Necesidad de registrar la actividad de usuarios y administradores sobre datos sensibles, ya que, aunque tengan acceso a las aplicaciones, solo deben consultar y acceder a los datos que estén relacionados con sus expedientes abiertos o quehaceres.
- Necesidad de salvaguardar estos logs en un servidor independiente, que tenga un número muy reducido de administradores de modo que, aunque se quieran borrar los rastros del acceso a información sensible, no les sea posible.

7.4.1 Selección de la solución

Los 2 requisitos son:

- Poder recibir de forma sencilla y universal los registros de varios servidores y dispositivos TIC.
- Poder proteger los logs recibidos para evitar su manipulación posterior.

Ante esta casuística la solución elegida ha sido instalar un servidor Red Hat (por disponer de guía de bastionado del CCN), sobre el que se ejecutará un servidor de Rsyslog, el cual volcará los datos a ficheros y cuando estos roten, se firmarán/cifrarán haciendo uso de GnuPG (GNU Privacy Guard).

Se han valorado otras alternativas como ELK o Graylog, ambas herramientas muy potentes, y que facilitarían enormemente la búsqueda de logs concretos, aunque tienen requisitos de potencia y complejidad altos y no permiten el firmado de forma nativa, por lo que han sido descartados.

Además, Rsyslog está muy extendido en todo el mundo y seguro que es compatible tanto con electrónica de red como con aplicaciones, facilitando la puesta en marcha e incorporación de nuevas fuentes.

Por último, en el caso de que en el transcurso de una investigación se deban analizar los datos mediante una interfaz amigable, siempre podrán importarse en alguna de las herramientas anteriores, y todo ello sin afectar a la recogida de nuevos registros.

7.4.2 Instalación y configuración de rsyslog

Debido a la casuística particular del servidor, éste deber ser administrado por el menor número de personas posibles (para que no puedan acceder a manipular los datos), por lo que se recomienda instalarlo en un servidor dedicado que no comparta funcionalidades con otros sistemas, de modo que sea lo más estanco posible.

Para documentar el caso, se parte de un servidor Red Hat Enterprise que ha sido bastionado siguiendo la guía CCN-STIC-610A22 del CCN, sobre el que se instalará Rsyslog utilizando la documentación oficial de Red Hat.

Los registros se recibirán en el puerto 514, para el cual se deberán permitir las conexiones entrantes en los cortafuegos que protejan dicho servidor.

Sobre dicho servidor se debe instalar el software Rsyslog y habilitarlo para que se inicie automáticamente mediante los siguientes comandos:

```
yum update
yum install rsyslog
systemctl enable rsyslog
```

La mayoría de las configuraciones sobre el servidor, se hacen en el fichero /etc/rsyslog.conf (configuración general) o en la carpeta /etc/rsyslog.d/ (casos particulares), tras cuyas modificaciones, se requiere que se reinicie el servicio mediante el siguiente comando:

```
systemctl restart rsyslog
```

Adicionalmente, tras cada cambio al fichero de configuración, se puede ejecutar el siguiente comando para validar que la sintaxis del archivo es correcta:

```
futro@futro:~$ rsyslogd -N 1
rsyslogd: version 8.2112.0, config validation run (level 1), master config /etc/rsyslog.conf
rsyslogd: End of config validation run. Bye.
futro@futro:~$
```

Ilustración 2 Comprobación de la configuración

Una vez revisadas las generalidades, se pasa a explicar la configuración del servicio:

Para empezar a recibir logs con una instalación sencilla que garantice la máxima compatibilidad, bastará con añadir las siguientes líneas al fichero de configuración (o descomentarlas si ya existen):

```
  GNU nano 6.2   /etc/rsyslog.conf *

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")
```

Ilustración 3 Configuración rsyslog UDP

Esta configuración permite la recepción de logs mediante UDP, con lo que se prioriza la recepción continua de registros sin necesidad de que la fuente verifique que estos llegan correctamente.

Si se prefiere utilizar TCP, bastaría con cambiar el módulo cargado del siguiente modo:

```
module(load="imtcp")
input(type=”imudp” port=”514”)
```

Si existieran varias interfaces de red, se pueden añadir dentro del campo input con la siguiente nomenclatura:

```
module(load="imtcp")
input(type=”imudp” port=”514” device="eth0")
```

Con los pasos anteriores únicamente se habilita la recepción de la información, pero para poder almacenarla en ficheros que se puedan firmar o cifrar, se deben crear reglas particulares.

En este caso, se documenta como crear un fichero de log por cada servidor del que se va a recibir la información, para lo que se necesita crear una “regla” por cada servidor. La identificación del servidor se hace en base a la dirección IP de origen de la conexión.

Para respetar la estructura de configuraciones de la aplicación, estas reglas se AÑADEN dentro del fichero 50-default.conf que se crea por defecto dentro de la carpeta /etc/rsyslog.d/.

Ejemplo de una regla, que guarda en /media/logs/rsyslog/servidor_padron.log los datos recibidos de la dirección IP 192.168.0.44, y en /media/logs/rsyslog/servidor_urbanismo.log los datos recibidos de la dirección IP 192.168.0.42:

```
  GNU nano 6.2                        /etc/rsyslog.d/50-default.conf
$template padron,"/media/logs/rsyslog/servidor_padron.log"
if $fromhost-ip=='192.168.0.44' then ?padron
& ~
$template urbanismo,"/media/logs/rsyslog/servidor_urbanismo.log"
if $fromhost-ip=='192.168.0.42' then ?urbanismo
```

Ilustración 4 Separación de los logs por servidores

Tras recargar el servicio, se comprueba que los logs están llegando, aunque de momento sin cifrar:

```
futro@futro:/var/log$ ll /media/logs/rsyslog/
total 28K
drwxr-sr-x 2 root  futro 4.0K Jun 12 01:29 ./
drwxrwsrwx 8 futro futro 4.0K Jun 12 01:08 ../
-rwxrwxrwx 1 root  root  7.3K Jun 12 01:30 servidor_padron.log*
-rwxrwxrwx 1 root  root  8.6K Jun 12 01:30 servidor_urbanismo.log*
```

Ilustración 5 Recepción de logs

Esta configuración tiene algunas particularidades:

- Se ha elegido recoger todo lo recibido de cada IP para evitar que haga falta configuraciones particulares en el servidor de origen.
- Si se desea separar diferentes aplicaciones de un mismo servidor en ficheros diferentes, en lugar de utilizar la variable $fromhost-ip, se puede utilizar $programname, o incluso combinar varias reglas mediante comandos AND y OR.
- Deliberadamente solo se registran los logs de los clientes registrados en el fichero de configuración, de modo que, aunque otros servidores enviasen sus

logs, no se recogerían, evitando saturar el disco duro, o la CPU por tener que codificar excesivos logs.

- No se ha contemplado la necesidad de que la comunicación sea autenticada ni cifrada, aunque existen opciones para ello. Si bien Rsyslog lo ofrece de forma nativa mediante una estructura de certificados digitales, establecer túneles ssh[13] entre los servidores de origen y destino, y enviar la información por dichos túneles resultaría más transparente para emisor y receptor, aportando más compatibilidad y permitiendo el envío seguro desde cualquier fuente.

7.5 Instalación y configuración de GnuPG y logrotate

De forma similar a rsyslog, se instala GnuPG y logrotate:

```
yum install logrotate
yum install gnupg
```

Se genera una clave GPG que quedará configurada en el sistema. Es importante hacerlo como root ya que logrotate se ejecutará con este usuario y de lo contrario no encontrará la clave publica o privada:

[13] Administración de servidores, Remo Suppi Boldrito. UOC (2023) Disponible en https://openaccess.uoc.edu/bitstream/10609/61265/2/Administraci%C3%B3n%20avanzada%20del%20sistema%20operativo%20GNU_Linux_M%C3%B3dulo2_Administraci%C3%B3n%20de%20servidores.pdf . Consultado el 12 de junio de 2023

```
root@futro:~# gpg --full-generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
  (14) Existing key from card
Your selection?
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072)
Requested keysize is 3072 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: Adrian
Email address:
Comment:
You selected this USER-ID:
    "Adrian"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
```

Ilustración 6 Generación clave gpg

Se averigua el key-id de la clave generada (D8E1226C):

```
root@futro:~# gpg --list-keys --keyid-format short
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
/root/.gnupg/pubring.kbx
------------------------
pub   rsa3072/D8E1226C 2023-06-12 [SC]
      E79CB06F20B824A0B08928E505846C49D8E1226C
uid         [ultimate] Adrian
sub   rsa3072/B56FC05F 2023-06-12 [E]

root@futro:~#
logout
```

Ilustración 7 Obtener key-id

El último paso será configurar logrotate para que use dicha clave:

Ilustración 8 Cifrado en logrotate

A continuación, se fuerza el rotado de los logs y se comprueba que efectivamente, además de rotar, se han cifrado con la clave privada volviéndose ilegibles e inalterables:

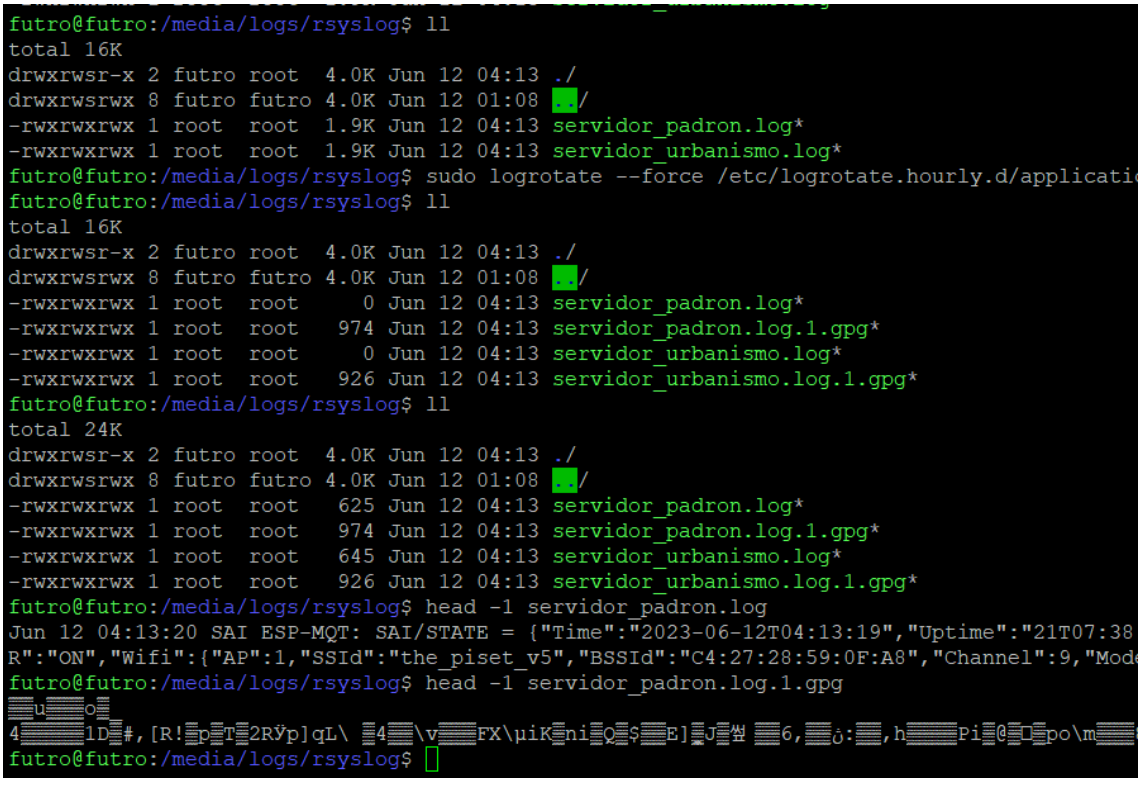


Ilustración 9 Comprobación del cifrado

Para concluir, cabe mencionar que, en lugar de cifrar los ficheros, se pueden crear ficheros de firma, para lo que, bastaría cambiar la configuración de logrotate del siguiente modo:

Ilustración 10 Firma de logs

7.6 Anexo V Política de control de accesos

Esta política documenta cómo se gestionan los accesos a los sistemas de información de CiudadX y a algunos de sus componentes auxiliares.

El documento es de aplicación por tanto a todos los usuarios de este, sean personal propio, personal subcontratado, así como los ciudadanos que hagan uso de alguno de los sistemas.

Dado que el documento es extenso y abarca varias casuísticas, su contenido íntegro es de obligado conocimiento para el personal de TI, mientras al resto de usuarios se les harán llegar los extractos de este que les apliquen, ya sea cuando reciban sus credenciales, cuando accedan a los sistemas, o cuando se establezca la relación contractual con el ayuntamiento, según corresponda.

Dado que el documento tiene relación directa con el cumplimiento del Esquema Nacional de Seguridad, se hace constar que da cumplimiento parcial a las siguientes medidas de seguridad y artículos de este:

- **Artículos** 12.6.e, 12.6.h y 20
- **Medidas de seguridad** org.3.4.a, op.pl.2, op.acc.1, op.acc.2, op.acc.4, op.acc.5, mp.if.1.2, pp.eq.3 y mp.com.3

7.6.1 Principios generales

Por defecto, **el acceso a todos los sistemas de información estará protegido**, al menos, con usuario y contraseña, u otras medidas de seguridad establecidas según el nivel de seguridad requerido por el sistema, contemplándose como excepciones, aquellos servicios públicos de consulta que dada su naturaleza no requieran de autenticación, como pueden ser el contenido público del portal web, la información de los kioscos digitales, sean interactivos o no, así como los equipos que se pongan a disposición del público para tareas que no requieran acceder a información no pública, como equipos de consulta de bibliotecas o redes wifi de cortesía.

Todas las contraseñas **deberán ser robustas**: siempre que el sistema lo permita, deberán tener al menos una longitud de 10 caracteres y combinar al menos 3 de los siguientes 4 tipos de dígito: mayúsculas, minúsculas, números y caracteres especiales. Cuando el sistema no permita cumplir con esta condición, se configurarán **mecanismos compensatorios**, como registro y reporte de todos los accesos, segundo factor de autenticación o acceso restringido solo desde ciertas ubicaciones. Estas medidas podrán ser modificadas en el momento de la toma de requisitos, o a petición formal del responsable de la misma.

Las cuentas se **bloquearán por inactividad**. El periodo de inactividad necesario para el bloqueo se definirá particularmente para cada sistema durante la fase de análisis y puesta en marcha de este. Una vez bloqueadas se notificará al responsable del empleado o responsable de la aplicación, según corresponda, para que valore la posible eliminación de la cuenta.

También **podrán ser bloqueadas** sin previo aviso en caso de sospecha fundada de **haber sido comprometidas** o utilizarse para fines maliciosos.

Cuando cualquier usuario reciba una credencial de acceso a alguno de los sistemas, junto con esta, se le **entregarán los deberes y obligaciones** que debe cumplir, incluida la custodia de las contraseñas en secreto, la obligación de reportar incidentes de seguridad y el extracto del presente documento que le aplique. Esta información deberá ser aceptada formalmente, ya sea mediante evidencia electrónica, o formulario en papel.

Dicha evidencia reflejará también que **el usuario ha recibido la credencial** y que desde ese momento se responsabiliza de ella.

En aquellos casos en que, debido al proceso de generación, la contraseña haya sido accedida por cualquier persona diferente al interesado, se **forzará el cambio** en su primer uso, haciéndose constar esta casuística en el documento de alta.

Previo a la entrega de una contraseña, se debe **comprobar la identidad del receptor.** Este requisito se considera cumplido si la entrega de la contraseña se hace por medio de algún sistema que ya requiera autenticación, como puede ser el gestor de incidentes o la sede electrónica.

Cuando un usuario tenga diferentes roles, dispondrá de **cuentas de usuario diferentes con diferentes permisos**. Algunos ejemplos son los administradores de los sistemas si también los operan, o los empleados públicos que también accedan como ciudadanos para sus gestiones personales.

Todo **intento de acceso será registrado** para su posible investigación ante un incidente de ciberseguridad. Este registro es extensible a la actividad de los usuarios en el uso de las aplicaciones, cuando así se haya definido en la toma de requisitos.

7.6.2 Tipos de acceso existentes y requisitos

Para establecer el nivel de seguridad a implantar, en la fase de toma de requisitos de cualquier nuevo sistema se analizará la naturaleza de la información que tratará, así como las posibles amenazas a las que estará expuesto, y, en consecuencia, se definirán las condiciones particulares. Estas pueden incluir, entre otros:

- Complejidad adicional de contraseñas
- Restringir el acceso a ciertos rangos de direcciones IP, horarios, usuarios, o combinación de los anteriores.
- Exigir doble factor de autenticación
- Establecer condiciones para bloqueo por intentos fallidos, o inactividad de usuario.
- Nomenclatura de las cuentas de acceso y forma de diferenciar las diferentes cuentas de un mismo usuario con varios perfiles.
- Fecha máxima de vida de una contraseña antes de ser cambiada
- Nivel de registro de intentos de inicio de sesión y actividad de usuario

Se contemplan diferentes tipos de acceso según los requisitos de seguridad de cada sistema:

- **Acceso mediante certificado digital**: será la forma exigida para acceder a la tramitación electrónica (principalmente mediante la sede electrónica), tanto por empleados del ayuntamiento como por los ciudadanos, con la particularidad de que los certificados instalados en los equipos corporativos requieren de una **contraseña** para poder habilitar el certificado.
- **Acceso mediante contraseña del dominio**: el ayuntamiento cuenta con un **dominio** corporativo, cuya cuenta habilita para poder acceder a los equipos de usuario, al correo electrónico, a la suite ofimática con su correspondiente funcionalidad cloud, y **a la mayoría de aplicaciones internas del ayuntamiento.** El acceso al dominio se hace mediante **usuario y contraseña** siempre y cuando se haga desde dentro de la red del ayuntamiento y desde un equipo dado de alta en el dominio.

- **Acceso mediante contraseña del dominio con doble factor de autenticación**: para accesos desde fuera de la red del ayuntamiento o con equipos no corporativos, se solicita un segundo factor de autenticación mediante aplicación móvil o llamada de verificación (en proceso de implantación).
- **Acceso mediante usuario y contraseña de aplicación**: aunque se prioriza el acceso a las aplicaciones mediante la cuenta del dominio, se contempla la posibilidad de acceder mediante usuario y contraseña a aquellos sistemas que por su particularidad lo requieran. Las condiciones de dicho acceso se establecerán en el momento de la toma de requisitos de este.

Por defecto, las **cuentas de acceso serán nominales**, personales e intransferibles, aunque se contempla la posibilidad de que por excepcionalidad técnica existan cuentas compartidas. El uso de estas cuentas debe estar autorizado por el responsable de seguridad, y su custodia correrá a cargo de los responsables de las aplicaciones o servicios a los que den acceso. El acceso a ellas se gestionará mediante el cauce habitual de gestión de incidentes, quedando reflejado en el registro de permisos, de modo que, ante una baja de usuario, sea posible identificar las contraseñas compartidas a las que ha tenido acceso y poder cambiarlas.

De igual modo, la custodia de las **contraseñas de aplicación** (contraseñas necesarias para que aplicaciones intercambien información entre sí), **las contraseñas maestras de dispositivos hardware**, o de administración de sistemas o bases de datos, estarán bajo la custodia de los responsables de los departamentos que las administran y siguiendo también el procedimiento de gestión de permisos.

7.6.3 Gestión de los permisos

Para proveedores y personal propio del ayuntamiento, existe un **registro de permisos de acceso** otorgados, el cual contiene varias asociaciones de entidades, implementando un modelo RBAC[14]:

1. Listado de usuarios con sus roles asignados
2. Listado de personal que puede autorizar la modificación de asignaciones a cada rol
3. Listado de roles, con los permisos que le otorgan
4. Listado de permisos extraordinarios de usuarios en sistemas concretos
5. Listado de personal que puede autorizar la modificación de permisos a cada sistema concreto

Este registro de permisos está enlazado al sistema de altas de nuevos usuarios y al sistema de peticiones de modificación de accesos del gestor de incidentes, de modo que cualquier cambio en los permisos de cada usuario, queda registrado automáticamente.

[14] Cloudflare (2023). Disponible en https://www.cloudflare.com/es-es/learning/access-management/role-based-access-control-rbac/ . Consultado el 13 de junio de 2023

7.6.4 Altas, bajas y modificaciones

Cuando un empleado o proveedor empiece a desarrollar sus funciones en el ayuntamiento, durante el proceso de alta el departamento de recursos humanos o contratación solicitará que se le cree una **cuenta inicial** de usuario en el dominio. El responsable inmediato del empleado o proyecto podrá solicitar que dicha cuenta tenga acceso a un listado de aplicaciones y sistemas preautorizados, los cuales se registrarán en el registro de permisos.

Para **cualquier cambio futuro** en los permisos de acceso a otros recursos, se utilizará el programa de gestión de incidentes en el cual se registrarán los cambios solicitados. Una vez autorizados, se concederán y se actualizará el registro de permisos.

Cuando RRHH o contratación detecten un cambio en la situación de los empleados o de los contratos del ayuntamiento con terceros, lo notificarán a los responsables para valorar si se deben anular o modificar los permisos de usuario, generalmente motivado por **cambios de departamento o bajas definitivas**.