MANUAL DE SEGURIDAD

Aplicaciones de Tramitación Telemática (Platea)

Nombre del archivo: Manual de Seguridad - v2.1 doc		
Páginas: 69		
Autor: DIT	***Revisado por:***	***Aprobado por:***
Fecha: 10-09-2010	***Fecha:***	***Fecha:***

Versión	**Fecha**	**Detalles**
1.0	04-06-2009	Primer borrador
2.0	25-06-2009	Versión revisada
2.1	10-09-2010	Corrección

Contenidos

0. Prólogo

Sustentado sobre los Servicios Comunes de Tramitación Telemática (SCTT), pilares básicos de la infraestructura técnica común para el desarrollo de la administración electrónica (e-Administración), de utilización obligatoria para todas las aplicaciones informáticas que sirvan de base a la tramitación telemática aparece el **Manual de Seguridad**. Este Manual de Seguridad dota a dicha infraestructura de una adecuada homogeneidad al establecer las medidas de seguridad de carácter general, así como de índole técnica y organizativa, dirigidas a asegurar el cumplimiento de las garantías de autenticidad, integridad, confidencialidad, disponibilidad, conservación de la información y trazabilidad.

El Manual de Seguridad queda dividido en dos apartados:

- **Política de seguridad**. Declaración de alto nivel de objetivos, directrices y compromiso de la Administración General de la Comunidad Autónoma del País Vasco y sus Organismos Autónomos para acometer la gestión de seguridad de la información en los medios electrónicos, informáticos y telemáticos utilizados en la prestación de servicios públicos.
- **Normativa de seguridad**. Medidas de seguridad de obligado cumplimiento. Es un compendio del conjunto de normas que soportan los objetivos recogidos en la política de seguridad de la información. En este nivel se describen los objetivos de seguridad y se anticipan las reglas generales de obligada adopción. Este apartado es el objetivo final perseguido por este documento.

1. Introducción

Uno de los activos más valiosos de la Administración General de la Comunidad Autónoma del País Vasco (en adelante, Administración General de la CAPV) y sus Organismos Autónomos es la información administrativa que trata para ofrecer servicios a sus ciudadanos. El presente Manual de Seguridad está enfocado al mantenimiento de la seguridad de la información de la Administración General de la CAPV y sus Organismos Autónomos, en el proceso telemático de la misma así como de los elementos que la tratan: **las aplicaciones informáticas que sirven de soporte a la tramitación telemática (e-Administración)**.

Dentro de este ámbito de aplicación, el presente documento trata la seguridad desde un punto de vista general, contemplando, además de la propia información, aspectos tales como el hardware, el software, las redes, los datos y el personal que manipula o da soporte a esta Infraestructura de Tramitación Telemática (en adelante, ITT).

La información puede encontrarse en tres estados fundamentales: transmisión, almacenamiento y proceso, y debe protegerse adecuadamente cualquiera que sea la forma que tome o los medios que se utilicen en dichos estados.

Asimismo, la información posee las siguientes características relacionadas con la seguridad (estas son las garantías que se deben salvaguardar para cualquier información o documentación en que se empleen medios electrónicos, informáticos y telemáticos ─en adelante, Medios EIT─):

- **Confidencialidad**: Característica que previene contra la puesta a disposición, comunicación y divulgación de información a individuos, entidades o procesos no autorizados.
- **Integridad**: Característica que asegura que la información no se ha transformado ni modificado de forma no autorizada durante su procesamiento, transporte o almacenamiento, detectando fácilmente posibles modificaciones que pudieran haberse producido.
- **Disponibilidad**: Característica que asegura que los usuarios autorizados tienen acceso a la información cuando se requiera y previene contra intentos de denegar el uso autorizado a la misma.
- **Autenticidad**: Característica por la que se garantiza la identidad del usuario que origina una información. Permite conocer con certeza quién envía o genera una información específica.
- **Conservación de la información**: En un sentido amplio, es el conjunto de procesos y operaciones que se conjugan para estabilizar y proteger los documentos del deterioro. A la hora de hablar de la gestión de recursos digitales, sea cual sea su forma o función, se debe tener en cuenta todas las etapas que componen el ciclo de vida de los documentos para aplicar las medidas de preservación lo antes posible. Por lo tanto, más que a una característica intrínseca de la información se hace referencia a la gestión del ciclo de vida de la información.
- **Trazabilidad**: Característica de la información que asegura el conocimiento de aspectos clave de las operaciones de creación, modificación y consulta, tales como: ¿quién realizó la operación?, ¿cuándo se realizó la operación?, ¿qué resultados tuvo la operación?

El objetivo del Manual de Seguridad desarrollado en el presente documento es el de establecer las directrices básicas y duraderas para la protección eficaz y eficiente, mediante

un enfoque preventivo, detectivo, reactivo y dinámico de uso de la información de la Administración General de la CAPV y sus Organismos Autónomos. Sólo de esta manera se conseguirá preservar la información de los ciudadanos, salvaguardando las garantías descritas y cumpliendo las leyes que afectan al tratamiento de la información.

Todo ello se desarrollará siguiendo y aplicando un principio de proporcionalidad, en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones. Asimismo sólo se requerirán a los ciudadanos aquellos datos que sean estrictamente necesarios en atención a la finalidad para la que se soliciten.

2. Ámbito de aplicación

El Gobierno Vasco dentro de su modelo de innovación y administración electrónica marca el establecimiento, puesta en funcionamiento, mejora y evolución de una infraestructura de e-Administración corporativa común para su utilización por parte del ciudadano y del Gobierno Vasco, así como el uso de dicha infraestructura desde otras iniciativas auspiciadas por la Administración para el tratamiento de la información propia de la Administración y la información generada por y para los ciudadanos.

Esta definición de organización orientada a la prestación de servicios al ciudadano, así como el uso de las nuevas tecnologías para la comunicación con los ciudadanos, suponen un reto para la Administración General de la CAPV y sus Organismos Autónomos, principalmente en el uso compartido de información y, por supuesto, en lo referente a la seguridad de dicha información.

En este ámbito, el reto es doble, ya que la Administración tiene la obligación de proteger la información de sus ciudadanos, así como de cumplir con las leyes emergentes que condicionan el uso de las tecnologías de la información – la Ley Orgánica de Protección de Datos de Carácter Personal, la Ley de los Servicios de la Sociedad de la Información, la Ley de Firma Electrónica, la Ley de Acceso Electrónico de los ciudadanos a los Servicios Públicos y el Decreto de Medios EIT –.

Con todo esto, el ámbito de aplicación del presente documento es:

- Aplicaciones del entorno de e-Administración (tal y como se entiende en el presente documento). Más concretamente a la infraestructura tecnológica PLATEA, componentes necesarios (elementos de red, servicios, equipos de usuario, periféricos, aplicaciones base) para el correcto uso de la misma; así como aquellas aplicaciones que hacen uso de dicha plataforma. A lo largo del presente documento se hará referencia a este conjunto de aplicaciones, componentes e infraestructura bajo la denominación ITT.
- La información afectada que será la tratada por la ITT, es decir, toda la información que utilizan, custodian o crean los empleados de la Administración General de la CAPV y sus Organismos Autónomos, tanto en soportes magnéticos, como ópticos, papel o cualquier otro soporte; bien resida en sus puestos de trabajo de forma local, como en servidores multiusuario, estén éstos ubicados o no en instalaciones propias.
- Procesos organizativos referentes al uso e implantación las aplicaciones de la ITT que afectarán a empleados de la Administración General de la CAPV y sus Organismos Autónomos.
- El público objetivo del presente Manual de Seguridad, desde un punto de vista funcional, será:
    - Funcionarios de la Administración General de la CAPV y sus Organismos Autónomos que hagan uso de la ITT.
    - Desarrolladores de las aplicaciones que dan soporte a la e-Administración. Por desarrollador se entiende cualquier persona que participa o tiene responsabilidad en el proceso de creación de la aplicación o infraestructura de las aplicaciones de la e-Administración. Los desarrolladores pueden ser propios o externos.
    - Administradores de recursos que dan soporte a la e-Administración. Por administrador se entiende cualquier persona que participa o tiene

responsabilidades en el correcto funcionamiento de la aplicación o la infraestructura de la e-Administración – administradores de sistemas, administradores de bases de datos, administradoras de red –. Los administradores pueden ser propios o externos.

- Otros que puedan desarrollar alguna función que afecte a las aplicaciones, su información, su infraestructura, las redes o las áreas de la e-Administración. Por ejemplo, las personas que se ocupan del mantenimiento de las áreas seguras.

- Desde un punto de vista contractual:
  - **Empleados**: personal funcionario, laboral y eventual
  - **Externos**: personal perteneciente a otras entidades que en virtud de relaciones especiales, como contratos de servicios, de asistencia técnica y de asesoría, entre otras, hace uso la Administración General de la CAPV y sus Organismos Autónomos.
- Se utilizará la primera clasificación (punto de vista funcional) para indicar el destinatario de cada medida de seguridad. La segunda clasificación (punto de vista contractual) se utilizará en el desarrollo de las medidas de seguridad.

3. Política de seguridad

Las directrices de la política de seguridad del Gobierno Vasco han sido definidas de acuerdo con el estándar ***ISO/IEC 27002:2005***[1]**,** que establece un marco de referencia de seguridad respaldado y reconocido internacionalmente. Este marco tecnológico, organizativo y procedimental de seguridad se soportará en un conjunto de normas o medidas, estándares, procedimientos y herramientas de seguridad para la protección de activos de información.

A continuación se exponen los diferentes dominios de seguridad que son cubiertos por la presente política y normativa de seguridad:

3.1. Política de seguridad

Este dominio proporciona las directrices generales de gestión y apoyo a la seguridad de la información en concordancia con los requerimientos del servicio al ciudadano y el marco regulatorio vigente. La Dirección establecerá claramente las directrices de la política en línea con los objetivos del servicio y demostrará su apoyo y su compromiso con la seguridad de la información a través de la publicación y mantenimiento de una política de seguridad de la información. Al ser un dominio de posicionamiento general respecto a la seguridad de la información, debe de cubrir todas las garantías definidas en la introducción: confidencialidad, integridad, disponibilidad, autenticidad, conservación y trazabilidad.

La Dirección de Informática y Telecomunicaciones (en adelante, DIT), con la participación de la Dirección de Innovación y Administración Electrónica y la Dirección de Atención Ciudadana, tiene la responsabilidad de elaborar el Manual de Seguridad en el ámbito de la e-Administración formado por políticas, normativas, estándares y procedimientos, con la finalidad de definir un marco de aplicación de la seguridad en el ámbito de las aplicaciones informáticas que sirven de soporte a la tramitación telemática que aseguren el cumplimiento de las garantías de seguridad – integridad, autenticidad, disponibilidad, confidencialidad, conservación y trazabilidad –. La presente Política de Seguridad establece las directrices generales de seguridad que se deben especificar en los subsiguientes componentes del Manual de Seguridad.

La DIT, como responsable de la elaboración del Manual de Seguridad, asume responsabilidad de la creación, la revisión periódica, la adecuación y el alineamiento de su contenido con los planes estratégicos del Gobierno Vasco. Adicionalmente, el Manual de Seguridad debe actualizarse considerando los cambios producidos en el marco legal vigente, inclusión de resultados relevantes de auditorías o análisis de riesgos, sugerencias de mejora al Manual de Seguridad, etc.

3.2. Aspectos organizativos de la seguridad de la información

Este dominio proporciona dos objetivos de seguridad: (1) gestionar la seguridad de la información dentro de la Administración y (2) mantener la seguridad de los recursos y de los activos de información que son accesibles por externos. Para la consecución del primer objetivo es importante que el Gobierno Vasco apruebe la política de seguridad de la información, asigne los roles de seguridad, coordine y revise la implementación de la seguridad en toda la Administración.

---

[1] *'Information technology – Code of practice for information security management',* correspondiente a la norma ISO/IEC 27002:2005.

Para la consecución del segundo objetivo es importante controlar cualquier acceso a la ITT y el procesamiento y comunicación de la información realizado por externos.

Al ser un dominio que versa sobre el cuidado y el control respecto al mantenimiento y seguimiento de implantación de la política de seguridad incidirá en las garantías de seguridad definidas en la introducción: confidencialidad, integridad, disponibilidad, autenticidad, conservación y trazabilidad.

El Gobierno Vasco proporciona unos medios organizativos para iniciar, conseguir y mantener la implantación de los objetivos de seguridad de la información en la Administración General de la CAPV y de sus Organismos Autónomos.

Dicha estructura organizativa debe estar formada por los responsables identificados en el Decreto 232/2007, de 18 de Diciembre:

- La titular del Departamento de Justicia y Administración Pública asume las funciones de aprobación de presente documento, que asegura la disponibilidad de los recursos dedicados a la seguridad de la información e informa del nivel de seguridad en las aplicaciones informáticas que sirven de soporte a la tramitación telemática.
- La DIT, según el Decreto de Medios EIT, tiene como función la elaboración del manual de seguridad dentro del ámbito de aplicación descrito.

Cualquier participación en el ciclo de vida de los proyectos que se lleven a cabo por la Administración General de la CAPV y sus Organismos Autónomos, en las aplicaciones informáticas que sirven de soporte a la tramitación telemática, requerirá la creación de equipos multidisciplinares, **de forma que la seguridad de la información sea tenida en cuenta en todas las fases de dicho ciclo de vida**.

Se realizarán revisiones independientes de las vulnerabilidades existentes, riesgos asociados y controles establecidos.

Adicionalmente a los requerimientos de funcionalidad, precio, rendimiento o capacidad, los contratos de prestación de servicios, por parte de externos, deben incluir requerimientos específicos de seguridad relativos a la tecnología y las actividades de aquellos que llevan a cabo su instalación, configuración, mantenimiento o eliminación.

De forma análoga, los contratos de externalización de servicios deben incluir requerimientos específicos de seguridad, relativos a la tecnología y las actividades de aquellos que llevan a cabo dichos servicios. Es responsabilidad del personal de la Administración entender los riesgos derivados del proceso de externalización y asegurar que existe una gestión eficaz de los mismos.

3.3. Gestión de activos

Este dominio proporciona una protección adecuada de los activos (incluyendo mantenimiento, inventario y clasificación), identificando a los propietarios de estos activos, cuya responsabilidad es el mantenimiento de los controles adecuados sobre los mismos. A tener en cuenta todos los medios o soportes que transmiten, almacenan y procesan información. Por ejemplo: los ordenadores portátiles, las comunicaciones móviles, y componentes de PLATEA. También se debe realizar una clasificación de los mismos ya que hay que asegurar que la información recibe un nivel de protección apropiado. La información debiera ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información. Este dominio tiene especial incidencia sobre la garantía de confidencialidad, aún así, es importante reseñar que la asignación de responsables por activo y el deber de éstos últimos de cumplir con las política de seguridad sobre estos activos hace que sea un dominio horizontal a las garantías de seguridad

definidas en la introducción: confidencialidad, integridad, disponibilidad, autenticidad y conservación de la información.

Se debe mantener un inventario de los activos de información de las aplicaciones informáticas que sirven de soporte a la tramitación telemática, velando porque exista un responsable y custodio para cada uno de los mismos. Este inventario debe ser actualizado de forma regular.

Con la finalidad de establecer un nivel de seguridad y tratamiento de la información adecuados, los activos de información deben ser clasificados de acuerdo a su sensibilidad y criticidad para la actividad de la e-Administración. Se deben elaborar las guías de clasificación de la información y las medidas de protección asociadas.

3.4. Seguridad ligada a los recursos humanos

Este dominio trata de asegurar que cualquier persona que tenga acceso a los activos inventariados dentro del ámbito de aplicación descrito (todos los empleados, tanto de Gobierno Vasco, de empresas subcontratadas, encargados del tratamiento y subcontratados de estos últimos) sepan y acepten sus responsabilidades en materia de seguridad de los sistemas de información y recursos con los cuales trabajan durante todo el ciclo de vida del empleado (antes de la contratación, durante la contratación y una vez finalizado la relación laboral). La principal garantía que se quiere cubrir es la confidencialidad mediante el uso de cláusulas referentes a obligaciones y responsabilidades del empleado. Otro de los objetivos es reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

El Gobierno Vasco proporcionará la formación apropiada a los usuarios en lo que respecta al presente Manual de Seguridad, incluyendo requerimientos de seguridad y responsabilidades legales.

Los usuarios deben de ser conscientes de la importancia de la seguridad en los sistemas de información del Gobierno Vasco. La seguridad eficaz depende, en parte, de que los usuarios sepan lo que se espera de ellos y cuáles son sus responsabilidades, comprometiéndose con las mismas. Éstos deben conocer los motivos de las medidas de seguridad física y lógica establecidas y también las consecuencias de violar la seguridad.

El Gobierno Vasco debe establecer un plan de comunicación que incluya sesiones de formación de seguridad para los empleados, que pueden realizarse como sesiones específicas o incluidas en reuniones que cubran otros aspectos relacionados. Estas sesiones podrán ser sustituidas por herramientas de formación distribuidas en soporte magnético o a través de la Intranet.

3.5. Seguridad física y ambiental

Este dominio trata de asegurar los activos físicos descritos (tangibles) a través del control de acceso y la protección contra contingencias externas (medioambientales). Las garantías que cubre este dominio son la disponibilidad, la integridad, la disponibilidad y la confidencialidad de la información.

La infraestructura que sustenta las aplicaciones informáticas que sirven de soporte a la tramitación telemática, así como los soportes de almacenamiento que éstos usan, que residan en sus edificios y en los proveedores de servicio o terceros, deben estar protegidos contra daño físico o hurto utilizando mecanismos de control de acceso físico que aseguren que únicamente el personal autorizado tiene acceso a los mismos.

Con esta finalidad, dicha infraestructura debe estar ubicada en áreas de acceso restringido, con diferentes niveles de seguridad, a las cuales únicamente pueda acceder personal debidamente autorizado. Los accesos a cada uno de los niveles deben ser registrados por mecanismos de control de acceso, quedando disponibles para posteriores auditorías.

Los sistemas y la información que soportan deben estar adecuadamente protegidos frente a amenazas físicas o ambientales, sean éstas intencionadas o accidentales.

3.6. Gestión de comunicaciones y operaciones

Este dominio trata de asegurar que la explotación de la infraestructura se realiza de forma segura y controlada, se supervisa su estado y se reportan incidencias. Para ello, define varios objetivos de control como: procedimientos y responsabilidades operacionales, gestión de servicios de terceros, planificación y aceptación de sistemas, protección contra código malicioso, copias de seguridad, gestión de la seguridad de red, gestión de dispositivos de almacenamiento, control sobre el intercambio de información entre sociedades, control de los servicios de comercio electrónico y monitorización de sistemas.. Este dominio detalla más controles técnicos que organizativos respecto a dominios anteriores. Las garantías que cubre son disponibilidad, confidencialidad, integridad y conservación de la información.

Se establecerán responsabilidades y procedimientos para la gestión y operación de todos los medios de tratamiento de información. Esto incluye elaborar de instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencias.

Se implantará la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso de la infraestructura deliberado o por negligencia.

Se requieren ciertas precauciones para prevenir y detectar la introducción de software dañino. El software y los recursos de tratamiento de información son vulnerables a la introducción de software dañino como virus informáticos, gusanos de la red, caballos de Troya y bombas lógicas. Los usuarios deben conocer los peligros que tiene el software dañino o no autorizado; y se deberán implantar controles y medidas especiales para detectar o evitar su introducción en puestos de trabajo, servidores y pasarelas de conexión a redes públicas o privadas necesarias para evitar la infección de los sistemas de información del Gobierno Vasco por virus o cualquier otro tipo de software dañino. En particular es esencial que se tomen precauciones para detectar o evitar los virus informáticos en los ordenadores personales. Es de obligado cumplimiento la actualización periódica y regular de los mecanismos antivirus para todo el Gobierno Vasco.

Se establecerán procedimientos rutinarios para conseguir la estrategia aceptada de respaldo haciendo copias de respaldo, ensayando su oportuna restauración, registrando eventos o fallos y monitorizando el entorno de los equipos cuando proceda.

La gestión de la seguridad de las redes que cruzan las fronteras de la Administración requiere una atención que se concreta en controles y medidas adicionales para proteger los datos sensibles que circulan por las redes públicas. Se deben establecer los controles necesarios que impidan la suplantación del emisor, modificación o pérdida de la información transmitida, tanto en las comunicaciones con sistemas situados en las redes internas, como con aquellos sistemas externos, independientemente de la plataforma, protocolos o aplicaciones que las soporten.

Se establecerán los procedimientos adecuados para proteger los documentos, soportes informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema frente a daño, robo y acceso no autorizado. El almacenamiento, manipulación, transporte, la destrucción o

desecho de cualquier activo de información del Gobierno Vasco, que contenga información sensible deberá garantizar la imposibilidad de acceso o recuperación de su contenido por parte de personal no autorizado.

Se controlarán los intercambios de información y software entre organizaciones, que deben cumplir con toda la legislación vigente. Se realizarán los intercambios sobre la base de acuerdos formales. Se establecerán procedimientos y normas para proteger los soportes en tránsito. Se considerarán las implicaciones de la seguridad asociadas al comercio, correo e intercambio de datos electrónicos (EDI, servicios de interoperabilidad), así como los requerimientos para las medidas y controles de seguridad.

Con la finalidad de asegurar la exactitud, relevancia y veracidad de los contenidos públicos del Gobierno Vasco, así como el cumplimiento de la legislación vigente relativa a la publicación de información en medios de difusión masiva, los procesos de publicación de contenidos deben utilizar una solución que provea una infraestructura de aprobación de los contenidos publicados.

Se debe crear la estructura organizativa multidisciplinar necesaria para acometer la resolución de incidentes de seguridad.

3.7. Control de acceso

Este dominio cubre uno de los aspectos más importantes y evidentes respecto a la seguridad: la problemática del control de acceso a los sistemas de información. Para ello plantea los siguientes objetivos de control: requisitos del negocio para el control de acceso, gestión de los accesos de los usuarios, responsabilidades del usuario, control de acceso de red, control de acceso del sistema operativo, control de acceso a las aplicaciones y a la información y teletrabajo y movilidad en el ámbito de la e-Administración. Las garantías que cubre este dominio son autenticidad y confidencialidad. También es el control base que asegure una buena trazabilidad.

Los permisos de acceso a las redes, sistemas y a la información que esos soportan se otorgarán de modo que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.

Se establecerán procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios. Estos procedimientos cubrirán todas las etapas del ciclo de vida del acceso a usuarios, desde el registro inicial de los nuevos hasta la baja del registro de los usuarios que ya no requieran dicho acceso a los sistemas y servicios. Se prestará especial atención si cabe al necesario control de la asignación de derechos de acceso privilegiados que permitan a ciertos usuarios evitar los controles del sistema.

Todos los accesos realizados a las aplicaciones informáticas que sirven de soporte a la tramitación telemática por los usuarios registrados llevarán asociado un proceso de identificación, autenticación y autorización. Se establecerán mecanismos de registro, monitorización de acceso y uso de los sistemas.

Las credenciales de acceso de cada usuario serán personales e intransferibles. Toda persona registrada que disponga de credenciales de acceso será responsable de mantener su confidencialidad y asegurar su correcto uso. Se establecerán los mecanismos necesarios en los sistemas para impedir la visualización de las credenciales por parte de terceras personas.

Debido a que una protección efectiva necesita la cooperación de los usuarios autorizados, los usuarios deben ser conscientes de sus responsabilidades en el mantenimiento de la efectividad de

las medidas de control de acceso, en particular respecto al uso de contraseñas y a la seguridad del material puesto a su disposición.

El acceso a los servicios desde redes externas e internas debe ser controlado de forma tal que se asegure que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios, por medio de:

- Interfaces adecuadas entre la red de la Administración General de la CAPV y sus Organismos Autónomos y las redes públicas o las privadas de otras Administraciones y/o Organizaciones.
- Mecanismos adecuados de autenticación para los usuarios y los equipos.
- Control de los accesos de los usuarios a los servicios de información.

El acceso remoto a *las* aplicaciones informáticas que sirven de soporte a la tramitación telemática desde redes públicas debe garantizar la confidencialidad de la información que se transmite, así como la identidad de los usuarios autorizados a hacer uso del servicio de acceso remoto mediante mecanismos de autenticación fuerte.

Se necesita restringir el acceso a los ordenadores para permitir sólo usuarios autorizados. Los ordenadores que atienden a múltiples usuarios deberían ser capaces de:

- Identificar y verificar la identidad de cada usuarios autorizado (y si procede, el terminal o la ubicación física del mismo).
- Suministrar mecanismos de gestión de contraseñas que garanticen la calidad de las mismas.
- Cuando proceda, restringir la conexión de usuarios o ventanas horarias.

Con la finalidad de detectar y reaccionar ante comportamientos sospechosos o inesperados, se debe establecer o activar sistemas de registro de actividades que almacenen los datos generados por las actividades de sistemas, aplicaciones y usuarios en los activos de información de la Administración General de la CAPV y sus Organismos Autónomos.

Se establecerán normativas, procedimientos y medidas técnicas específicas para la protección de sistemas portátiles y accesos remotos de teletrabajo.

3.8. Adquisición, desarrollo y mantenimiento de los sistemas de información

Este dominio trata de asegurar que la seguridad es una parte que está integrada en los sistemas de información. Para ello establece varios objetivos de control: requisitos de seguridad que afectan a los sistemas de información (sean adquiridos o desarrollados), correcto procesamiento de las aplicaciones, controles criptográficos, seguridad en los sistemas de ficheros, seguridad en los procesos de desarrollo y soporte y gestión de vulnerabilidades técnicas. Este dominio trata de cubrir las garantías de disponibilidad, confidencialidad e integridad.

Los proyectos de desarrollo que se inicien en la Administración y afecten directamente a las aplicaciones informáticas que sirven de soporte a la tramitación telemática deben llevarse a cabo considerando **requisitos específicos de seguridad durante todo su ciclo de vida**.

El desarrollo y mantenimiento de las aplicaciones dentro del ámbito especificado debe incluir los controles y registros apropiados que garanticen la correcta implementación de las especificaciones de seguridad y se llevará a cabo teniendo en cuenta las mejores prácticas de seguridad en la programación.

Especialmente, se usarán sistemas y técnicas criptográficas –cifrado, firma digital, no-repudio– para proteger la información sometida a riesgo, cuando otras medidas y controles no proporcionen la protección adecuada.

La información residente en las aplicaciones informáticas que sirven de soporte a la tramitación telemática debe estar protegida contra modificaciones no autorizadas empleando mecanismos que aseguren la integridad de la misma.

Se debe proveer de las guías, estándares, recomendaciones y procedimientos necesarios para facilitar la inclusión de la seguridad durante las etapas del ciclo de vida de desarrollo, tales como uso de controles criptográficos, gestión de claves, programación segura, etc.

Los entornos que forman parte del ciclo de vida de desarrollo informático deben estar convenientemente separados o segmentados en todos y cada uno de los sistemas. Asimismo, y con la finalidad de evitar el acceso o divulgación de datos que residan en los entornos, se debe controlar el intercambio de datos reales entre el entorno de producción y el resto de entornos.

En los entornos de pruebas o desarrollo, para las aplicaciones, o infraestructura deben estar disponibles juegos de datos de prueba, preparados específicamente, donde las relaciones entre datos y personas hayan sido disociadas o enmascaradas.

3.9. Gestión de incidentes de seguridad de la información

Este dominio trata de garantizar que los eventos y debilidades en la seguridad asociados a la ITT y las aplicaciones soporte de la e-Administración sean comunicados para, de este modo, poder realizar las acciones correctivas oportunas y adecuadas. Este es un dominio que está enfocado principalmente a cubrir las garantías de disponibilidad, confidencialidad e integridad.

Se debe exigir que se informen con la mayor celeridad posible (ante cualquier debilidad observada o sospecha). Para cumplir este objetivo hay que establecer los procedimientos y cauces adecuados (canales de gestión conocidos); este punto esta ligado con el apartado 3.4 (sobre la seguridad ligada a recursos humanos), en el apartado sobre concienciación, formación y capacitación en seguridad de la información.

Así mismo, se debe garantizar que se aplica una metodología sólida para la gestión de incidentes de seguridad (establecer responsabilidades y procedimientos), a la vez que emplear procesos de mejora continua y métodos para la recogida de evidencias.

Existe un mecanismo que permite la monitorización de las incidencias de seguridad, cuantificación y costes asociados de las mismas, así como la recopilación de evidencias.

Se establecerán procedimientos formales para informar y priorizar eventos de seguridad. Todo el personal afectado deberá conocer los procedimientos para informar de los diferentes tipos de eventos y debilidades que pudieran impactar en la seguridad de las aplicaciones informáticas que sirven de soporte a la tramitación telemática.

Se establecerán responsabilidades y procedimientos formales para manejar los eventos de seguridad y debilidades con eficacia una vez que éstas hayan sido comunicadas. Además, se establecerá un proceso formal de mejora continua sobre toda la gestión de incidentes de seguridad.

Se recopilarán las evidencias necesarias por cada incidente con el fin de cumplir con la legalidad vigente.

3.10. Gestión de la continuidad del servicio

Este dominio trata de asegurar la disponibilidad de la ITT que soporta las aplicaciones de la e-Administración en caso de catástrofe. El objetivo es establecer un plan de acción para minimizar los efectos de una catástrofe. Las garantías que este dominio cubre son la integridad, la disponibilidad y la conservación de la información.

El objetivo es establecer un proceso de gestión de continuidad de actividad para garantizar la recuperación de los procesos críticos de la Administración General de la CAPV y sus Organismos Autónomos en caso de desastre, reduciendo el tiempo de indisponibilidad a niveles aceptables, desde el punto de vista de la actividad de la Administración, mediante la adecuada combinación de controles de carácter organizativo, tecnológico y procedimental, tanto preventivos como de recuperación.

Este proceso se desarrollará mediante un Plan de Continuidad del Servicio que debe ser probado de forma periódica y regular y que se debe mantener actualizado en todo momento. Para ello, se debe evaluar el riesgo y el impacto asociado ocasionado por la ausencia de continuidad de los sistemas de información que den soporte o estén implicados en la actividad del Gobierno Vasco.

3.11. Cumplimiento

Este dominio trata de evitar el incumplimiento del marco normativo y cualquier requerimiento de seguridad que éste obligue mediante el cumplimiento en los sistemas de información de las políticas y estándares de seguridad desarrollados a través del presente Manual de Seguridad. También trata de maximizar la efectividad del proceso de auditoría de la infraestructura y las aplicaciones de la e-Administración. Este dominio es horizontal y cubriría las garantías definidas en la introducción: confidencialidad, integridad, disponibilidad, autenticidad y conservación de la información.

El Gobierno Vasco adquiere para con sus ciudadanos la responsabilidad de cumplir con la legislación vigente relativa a la seguridad de la información. Se debe identificar los estatutos relevantes, regulaciones, leyes y requisitos contractuales relativos a seguridad de la información que afecten directa o indirectamente a la seguridad de los activos de información de las aplicaciones de la e-Administración.

Es responsabilidad de todas las áreas implicadas conocer y cumplir la legislación vigente de aplicación en sus ámbitos de actuación.

Específicamente, se deben contemplar los mecanismos y procedimientos indicados por la Ley Orgánica de Protección de Datos de Carácter Personal y el Reglamento de Medidas de Seguridad asociado, debido a que es el marco legislativo de referencia de seguridad de la información de carácter personal.

El personal del Gobierno Vasco adquiere el deber de secreto, es decir, la responsabilidad de no divulgar ningún tipo de información que haya adquirido en la realización de su trabajo.

Las aplicaciones informáticas que sirven de soporte a la tramitación telemática se deben someter periódicamente a una auditoría, encargada de verificar el cumplimiento de la normativa de seguridad y de los procedimientos e instrucciones vigentes en materia de seguridad de la información.

El proceso de auditoría debe verificar el cumplimiento de las iniciativas de seguridad planificadas a corto plazo, realizar periódicamente revisiones del grado de instauración de los controles y de su

efectividad desde el punto de vista de la seguridad y ser independiente de las comprobaciones realizadas internamente por el Gobierno Vasco.

Se establecerán las medidas necesarias para evitar la desactivación, accidental o malintencionada, de los mecanismos de seguimiento y auditoría.

Se realizarán revisiones regulares en cuanto a la seguridad de la ITT y de las aplicaciones de la e-Administración.

3.12. Gestión de la seguridad

Dentro del ámbito de aplicación se establecerá un Sistema de Gestión de la Seguridad de la Información (en adelante, SGSI) basado en el estándar UNE-ISO/IEC 27001:2007 (ISO/IEC 27001:2005) con el objetivo de establecer un proceso de mejora continua de la seguridad.

Para ello se realizarán revisiones periódicas, al menos una vez al año, en la que se llevará a cabo la revisión del alcance del SGSI entre otras acciones.

Estas revisiones también se realizarán en respuesta a cualquier evento que pusiese afectar al alcance del SGSI, como:

- Cambios de legislación.
- Cambios en la organización.
- Cambios del entorno técnico.
- Incidencias que puedan afectar a la gestión del SGSI.

El objetivo de estas revisiones será:

- Conocer en que nivel afecta el evento al alcance del SGSI.
- Modificar el alcance, si procede.
- Definir e implementar un nuevo SGSI, si procede.

Las reuniones podrán tener carácter físico o virtual, disponiéndose de un repositorio centralizado donde se recogerán las actas, propuestas y decisiones que afecten al SGSI.

4. Desarrollo Normativo

4.1. Explicación de las fichas

El desarrollo de las medidas de seguridad se realiza mediante fichas. Las medidas de seguridad se aplicarán para alcanzar la seguridad debida y proporcionada a la categoría del sistema de información a proteger, el tipo de activos que constituyen el sistema a proteger y las dimensiones de seguridad relevantes en el sistema a proteger. Por todo ello, cada ficha dispone de los siguientes campos:

- **Medida**: nombre de la medida.
- **Código**: referencia unívoca.
- **Objetivo**: relaciona la medida con un apartado de la política de seguridad.
- **Alcance**: indica la obligatoriedad de adopción de la medida;
    - Las fichas clasificadas como “bajo”, color verde, indican que la medida de seguridad debe ser aplicable a todos los sistemas de información.
    - Las fichas clasificadas como “medio”, color amarillo, indican que la medida de seguridad debe de ser aplicable a sistemas de información que dispongan de una clasificación media.
    - Las fichas clasificadas como “alto”, color rojo, indican que la medida de seguridad debe de ser aplicable a sistemas de información que dispongan de una clasificación alta.
- **Garantías**: indica las garantías de seguridad que cubre la medida de seguridad.
- **Destinatarios**: roles funcionales que deberían de tener en cuenta la medida de seguridad.
- **Desarrollo**:
    - El texto de la medida se subdivide a su vez en:
        - Un “propósito” que define el objetivo de la medida de seguridad.
        - Una “exposición” que desarrolla la medida de seguridad en sí.
        - Una “actividad” de seguridad en el caso de que la medida lo requiera. El conjunto de actividades formarán parte de los procedimientos de seguridad (ver medida de seguridad M-2-2).

4.2. Índice de fichas

M-3	Gestión de activos
M-3-1	Uso y responsabilidad sobre los activos
M-3-2	Tratamiento de la información
M-4	Seguridad ligada a los recursos humanos
M-4-1	Caracterización del puesto de trabajo
M-4-2	Responsabilidades de dirección, formación y concienciación
M-5	Seguridad física y ambiental
M-5-1	Áreas seguras – control de acceso
M-5-2	Áreas seguras – seguridad medioambiental
M-5-3	Seguridad en equipos
M-6	Gestión de comunicaciones y operaciones
M-6-1	Segregación de funciones
M-6-2	Planificación de los cambios
M-6-3	Protección frente a código dañino
M-6-4	Seguridad en los servicios de red
M-6-5	Manipulación de los soportes
M-6-6	Copias de seguridad
M-6-7	Canales de comunicación
M-6-8	Protección de servicios y aplicaciones Web
M-6-9	Planificación del sistema
M-6-10	Supervisión
M-6-11	Transporte
M-7	Control de acceso
M-7-1	Proceso de autorización / Acceso de usuario
M-7-2	Control de acceso
M-7-3	Acceso a red
M-7-4	Responsabilidades de usuario
M-8	Adquisición, desarrollo y mantenimiento de los sistemas de información
M-8-1	Requisitos de seguridad
M-8-2	Criptografía
M-8-3	Aceptación y puesta en servicio
M-9	Gestión de incidentes de seguridad de la información
M-9-1	Gestión de incidencias
M-10	Gestión de la continuidad del servicio
M-10-1	Medios alternativos
M-10-2	Continuidad de servicio

M-10-3	Planes de continuidad de servicio que incluyan seguridad de la información
M-10-4	Pruebas periódicas
M-11	Cumplimiento
M-11-1	Cumplimiento legal
M-11-2	Cumplimiento técnico
M-12	Gestión de la seguridad
M-12-1	Análisis de riesgos
M-12-2	Mejora continua

Medida	Código	Objetivo	Alcance
Política de seguridad	M-1-1	Política de seguridad	Bajo
Garantías	**Destinatarios**		
Todas las garantías de seguridad	Todos los usuarios		

Desarrollo

Propósito

Recoger el posicionamiento de la Administración General de la CAPV y Organismos Autónomos en materia de seguridad en el ámbito descrito para el presente documento.

La política de seguridad requiere un alto compromiso de la Administración, competencia para establecer fallos y debilidades y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas y a los sistemas de información.

Exposición

Por tanto, se deben proporcionar indicaciones sobre la gestión de la seguridad de la información dentro de la ITT. Esto es:

- Este documento, el Manual de Seguridad, enuncia el compromiso del Gobierno Vasco (Administración General de la CAPV y sus Organismos Autónomos) en dicho ámbito y establece el enfoque para manejar la seguridad de la información.
- La política de seguridad debe ser revisada a intervalos concretos y periódicos de tiempo o cuando se produzcan cambios significativos que la afecten con el fin de mantener la idoneidad, adecuación y eficacia.
- La política de seguridad debe ser recogida en un documento que debe ser aprobado y comunicado.

Actividades

- Elaboración y mantenimiento de la política de seguridad

Medida	Código	Objetivo	Alcance
Contratación y acuerdos de nivel de servicio	M-2-1	Aspectos organizativos de la seguridad de la información	Medio

Garantías	Destinatarios
Autenticidad, integridad, disponibilidad, confidencialidad, trazabilidad y conservación	Funcionarios

Desarrollo

Propósito

Cubrir todos los aspectos de seguridad pertinentes en los acuerdos con terceros, que conlleven algún tipo de acción sobre la ITT.

Exposición

- Es prioritario mantener la seguridad de la ITT que pueda ser manejada por externos. Para ello es importante gestionar la seguridad desde el momento que se formalizan los contratos con externos en dicho ámbito. Esto es:
  - Antes de acordar el acceso de externos, se debe identificar cuáles son los principales riesgos de seguridad de los activos de la ITT que se van a manejar para formalizar las medidas concretas más acordes a cada casuística concreta. La adopción de dichas medidas quedará reflejada y formalizada en el contrato que se realice con el externo.
  - Incluir análisis de riesgos de los activos.
  - Los acuerdos o contratos con externos que involucran el acceso a los activos de la ITT, o agregan productos/servicios/otros a la misma deben abarcar todos los requerimientos de seguridad que establece el Manual de Seguridad.
  - Además, se desarrollarán Acuerdos de Nivel de Servicio (en adelante, ANS o SLA en sus siglas en inglés) con el fin de fijar y formalizar el nivel de calidad de servicio acordado.

Actividades

- Gestión de ANS con externos

Medida	Código	Objetivo	Alcance
Procedimientos de seguridad	M-2-2	Aspectos organizativos de la seguridad de la información	Bajo

Garantías	Destinatarios
Autenticidad, integridad, disponibilidad, confidencialidad, trazabilidad y conservación	Todos los usuarios

Desarrollo

Propósito

Definir claramente todas las responsabilidades relativas a la seguridad de la información.

Exposición

- Todas las responsabilidades en el ámbito descrito de seguridad deben estar claramente definidas.
  - La asignación de las responsabilidades en el ámbito descrito de seguridad debe realizarse en concordancia con la política de seguridad definida.
  - Se deben definir claramente las responsabilidades para la protección de los activos y para llevar a cabo los procesos de seguridad.
  - Cuando se considere necesario, esta responsabilidad debe ser complementada con un alineamiento más detallado para áreas y medios de procesamiento de información específicos.
  - Desde el Gobierno Vasco se deben definir claramente las responsabilidades que la Administración General de la CAPV y sus Organismos Autónomos debe tomar para la protección de los activos y en base a las medidas del presente Manual de Seguridad.
- Se debe proponer un Responsable de Seguridad General para la ITT que asuma la tarea general del desarrollo y la implementación de la seguridad y fundamente la identificación de medidas de seguridad. Dentro de la tarea general del desarrollo y la implementación de la seguridad se pueden destacar estas áreas que deberán estar asignados a un responsable funcional:
  - Elaboración y mantenimiento de la política de seguridad.
  - Gestión de ANS.
  - Definición de responsabilidades y segregación de funciones.
  - Gestión del ciclo de vida del activo.
  - Clasificación de la información.
  - Gestión de la formación en seguridad.
  - Gestión de la securización de equipos informáticos.
  - Gestión de soportes.
  - Gestión de incidencias.
  - Gestión de registros de auditoría.
  - Gestión de identidades y accesos
  - Gestión de la seguridad en el ciclo de vida de desarrollo.
  - Ciclo de vida de certificados
  - Gestión de la continuidad del servicio.
  - Gestión de auditorías de seguridad.
  - Administración del Sistema de Gestión de la Seguridad.
- Los trabajos de dichas áreas se acometerán dentro de un marco de trabajo orientado a procesos.

Con esta forma de trabajo será más sencillo implementar una segregación de funciones efectiva según medida *M-6-1*.

- Se deberá introducir en todos lo ámbitos de la seguridad donde sea posible la segregación de funciones con el fin de que nadie pueda tener acceso, modificar o utilizar los activos sin autorización o detección. Se debiera separar la iniciación de un evento de su autorización y se debiera considerar la posibilidad de colisión en el diseño de los controles.

Medida	Código	Objetivo	Alcance
Uso y responsabilidad sobre los activos	M-3-1	Gestión de activos	Bajo
Garantías	**Destinatarios**		
Autenticidad, integridad, disponibilidad, confidencialidad y conservación	Todos los usuarios		

Desarrollo

Propósito

Conseguir y mantener la protección necesaria de los activos de la ITT. Para ello se elaborará un inventario y se definirán normas y responsabilidades sobre usos aceptables de los mismos.

Exposición

- Se debe elaborar un inventario completo y actualizado de todos los activos de la ITT.
  - Para elaborar dicho inventario se deben dividir los activos (ver definición de activo según ISO) en categorías definidas formalmente.
  - Cada activo debe tener recogido en dicho registro la información necesaria que consiga identificarlo, describirlo, clasificarlo y ubicarlo. Asimismo, se deberán determinar los propietarios de activos y la especificación de las responsabilidades adquiridas por éstos.
  - Habrá que desarrollar e implantar los procedimientos que permitan clasificar, etiquetar y mantener los activos de la ITT.
  - Se deberá definir y ejecutar periódicamente, al menos una vez al año, un proceso de seguimiento de la completitud y veracidad del mismo, identificando y actualizando el registro de las modificaciones realizadas sobre él; con el objeto de asegurar la integridad del inventario.
- Se debe asegurar la disponibilidad del inventario a disposición de todos los responsables del mismo quiénes, a su vez, tienen la obligación de mantener actualizados los datos del mismo.

Actividades

- Ciclo de vida del activo

Medida	Código	Objetivo	Alcance
Tratamiento de la información	M-3-2	Gestión de activos	Bajo
Garantías	**Destinatarios**		
Integridad, disponibilidad, confidencialidad y conservación	Todos los usuarios		

Desarrollo

Propósito

Asegurar que la información recibe un nivel adecuado de protección. Para ello se establecerán directrices de clasificación y mecanismos de etiquetado y manipulación.

Exposición

- Toda la información tratada desde la ITT, debe estar clasificada de acuerdo a criterios de confidencialidad, relevancia y criterios derivados de la gestión del riesgo de la información.
- En función de la clasificación que se realice de la información, se deben cumplir una serie de requisitos con el objetivo de asegurar su manejo.
- Los datos de carácter personal, independientemente de la categoría en la que queden incluidos, deben cumplir las disposiciones recogidas en la legislación vigente respecto a la protección de datos de carácter personal.

Actividades

- Clasificación de la información

Medida	Código	Objetivo	Alcance
Caracterización del puesto de trabajo	M-4-1	Seguridad ligada a los recursos humanos	Medio
Garantías	**Destinatarios**		
Confidencialidad	Todos los usuarios		

Desarrollo

Propósito

Formalizar las funciones y responsabilidades de los empleados y externos conforme a la política descrita en el presente documento. Con ello se pretende que toda persona afectada entienda sus responsabilidades y que éstas se formalicen previamente a la definición del puesto de trabajo y se hagan tangibles mediante un contrato.

Exposición

- Los empleados y externos podrán utilizar los activos de la ITT exclusivamente para el desempeño de las funciones que estos tengan asignadas. Se deberá asegurar que dichas funciones estén debidamente reflejadas en los perfiles y accesos que se soliciten para el uso/acceso de/a los mismos. Considerando de especial observancia la aplicación del marco legal relacionado con el tratamiento de los datos de carácter personal y a cualquier otro dato que esté sujeto a legislación o regulación vigente, estarán cumpliendo con las medidas en torno a la ITT.
- Las responsabilidades referentes a la seguridad de la información estarán incluidas en las condiciones de empleo de cada uno de los trabajadores, debiéndose verificar el cumplimiento de las mismas.
- Los externos deberán firmar dichas condiciones de empleo como parte de sus términos o condiciones iniciales de trabajo, comprometiéndose de esa forma a no divulgar la información a la que pudiesen tener acceso, incluso después de finalizada su relación laboral.
- En caso de incumplimiento de las condiciones de empleo aceptadas se podrán iniciar las acciones administrativas y/o penales correspondientes.

Actividades

- Definición de responsabilidades y segregación de funciones

Medida	Código	Objetivo	Alcance
Responsabilidades de dirección, formación y concienciación	M-4-2	Seguridad ligada a los recursos humanos	Bajo
Garantías	**Destinatarios**		
Confidencialidad	Todos los usuarios		

Desarrollo

Propósito

Asegurar que todos los empleados y externos son conscientes de las amenazas y problemas que afectan a la seguridad de la ITT y de sus responsabilidades y obligaciones. Para ello es clave que empleados y externos estén preparados para cumplir con la política establecida en este ámbito y, de esta forma, reducir los problemas que tengan un origen en el error humano.

Exposición

- La dirección de la Administración General de la CAPV y sus Organismos Autónomos debe ser sensible con los temas de seguridad. Para ello deberá de desplegar los mecanismos necesarios para implementar las medidas de seguridad necesaria y de auditoría, reporting y control.
- La dirección debe de promover la divulgación y el conocimiento de las medidas de seguridad como paso fundamental para la concienciación en dichos temas y de poner los medios formativos necesarios a los que desarrollen o ejecuten las actividades de seguridad presentes.
- Todos los empleados y externos deberán solicitar y recibir la formación adecuada en materia de seguridad de la información con el objetivo de cumplir las normas, estándares, y otras directrices definidas en el presente Manual de Seguridad.
- Dicha formación abarcará igualmente los requisitos de seguridad, responsabilidades legales, objetivos de control, así como las buenas prácticas en el uso correcto de los activos de la ITT. Los empleados, en sus planes formativos, dispondrán de la formación necesaria. Para externos, la propia empresa deberá de inculcar los aspectos necesarios a sus empleados.

Actividades:

- Planificación de formación en seguridad

Medida	Código	Objetivo	Alcance
Áreas seguras – control de acceso	M-5-1	Seguridad física y ambiental	Bajo
Garantías	**Destinatarios**		
Integridad, confidencialidad y disponibilidad	Todos los usuarios		

Desarrollo

Propósito

Prevenir los accesos físicos no autorizados y las intromisiones en las instalaciones y, por tanto, en la información de la organización.

Por **Áreas Seguras** se entiende que son las salas dedicadas para el albergue de la ITT. También abarca las zonas físicas y públicas de la e-Administración. Debido a la diversa naturaleza de los activos implicados, el albergue de la ITT se encuentra muy disgregado (varias localizaciones, varias casuísticas) y en ocasiones algunos activos de la ITT compartirán ubicación con activos de otros orígenes. Con lo cual no se pueden definir medidas específicas en el ámbito de la ITT sino que se deberán adoptar muchas de carácter general.

Exposición

Medidas generales (que aplican a la ITT aunque no se han definido explícitamente para la misma).

Sobre salas de albergue de servidores:

- Se tratará, preferentemente, de salas dedicadas. En el caso de tratarse de salas compartidas con otros usos, éstas no requerirán un acceso frecuente por parte del personal.
- Las salas permanecerán cerradas siempre que no se encuentre personal en su interior.
- Sólo tendrán autorización de acceso los responsables de aquellos activos (equipamientos) que se alojen en su interior, el responsable de su administración o mantenimiento, los servicios de vigilancia y aquellos otros a quienes éstos hubieran autorizado explícitamente.

Sobre los edificios (instalaciones) y el acceso a los mismos:

Toda instalación (incluidas las instalaciones externas a la Administración), debe estar dotada con aquellos mecanismos de seguridad física que permitan:

- Impedir el acceso a personas no autorizadas a las zonas seguras donde se procese o almacene información.
- Asegurar la protección de los recursos informáticos. Ver M-5-2.

Por tanto, será preciso definir un perímetro de seguridad física dentro del cual se debe ubicar la ITT. El perímetro de seguridad debe comprender tanto barreras físicas de seguridad como mecanismos de control de acceso apropiados.

Sobre las barreras físicas:

- El perímetro de los edificios que contengan recursos de tratamiento de información deberá tener la solidez física suficiente que evite entradas no autorizadas, mediante muros externos y las protecciones de las puertas y ventanas.
- Estas medidas se podrán complementar con el uso de mecanismos de control, alarmas, verjas y cierres en los diversos puntos de acceso al edificio, incluidas ventanas. Estos mecanismos incrementarán la robustez del perímetro de seguridad de dichos edificios, de acuerdo a los requisitos de seguridad de la información.

Sobre los mecanismos de control de acceso:

- Se deberán controlar adecuadamente las zonas de carga y descarga de los edificios.
- Se definirán los requisitos específicos para garantizar la seguridad dentro de las oficinas administrativas, abiertas al público o no, las salas de servidores y centros de explotación, zonas

de archivo, salas de equipamiento eléctrico o comunicaciones, y cualquier otra zona que en virtud del activo albergado deba ser considerada como segura. Por tanto, el control de acceso deberá ser acorde con la clasificación de los activos y la función de tratamiento que en ellas se desarrolle.

- En las zonas dotadas de control de acceso, los permisos de acceso y permanencia que se otorguen, se establecerán en función de las necesidades derivadas de la actividad profesional.
- Se deberá mantener actualizada en todo momento, una lista de las personas con permiso de acceso por zonas. Los accesos temporales a las distintas zonas, incluyendo los accesos fuera de horario habitual, deberán ser expresamente autorizados.
- Los accesos (entradas y salidas) serán registrados por el mecanismo de control de acceso que corresponda.
- Toda persona deberá portar, permanentemente y en lugar visible, mientras permanezca en las instalaciones, un identificador.
- El personal de mantenimiento y limpieza será tratado a efectos de acceso al igual que el resto de personal autorizado.
- Además de los sistemas de información y comunicaciones (servidores), los soportes de almacenamiento que residan en edificios propios o en los de los externos deberán estar protegidos contra daño físico o hurto, utilizando mecanismos de control de acceso físico que aseguren que únicamente personal autorizado tiene acceso a los mismos.
- Queda expresamente prohibido manipular los mecanismos de control de acceso, provocando su incorrecto funcionamiento, como por ejemplo obstaculizando el correcto cierre de las puertas.
- Dependiendo del tipo de activos que contenga el área segura, se aplicarán controles de acceso específicos y acordes al riesgo que se pretenda evitar.
- El equipamiento que forma parte de los sistemas de información y comunicaciones de la Administración no deberá ser sacado fuera de sus instalaciones sin la previa autorización por parte del responsable del activo.
- Cuando haya necesidad de sacar temporalmente algún elemento que forme parte de los sistemas de información y comunicaciones fuera de las instalaciones a las que dicho elemento esté adscrito, se deberá registrar su salida. Cuando el elemento retorne a su ubicación, se cerrará el registro que fue abierto a su salida.
- Así mismo, toda entrada de equipamiento que se produzca en las instalaciones de la Administración deberá ser registrada con el fin de controlar dicho equipamiento.
- Se deberán hacer controles periódicos o de inventario del equipamiento existente, con el fin de detectar posibles sustracciones, paliar el posible daño que las mismas puedan causar, y depurar las responsabilidades a que diesen lugar.

Sobre armarios y otros contenedores de oficina:

- En el caso que se trate de armarios ubicados en zonas de oficina, éstos serán adecuados a la naturaleza del equipamiento albergado, estarán cerrados con llave, y para su ubicación se evitarán zonas de paso u oficinas administrativas abiertas al público.

Actividades

- Autorización de acceso físico.

Medida	Código	Objetivo	Alcance
Áreas seguras – seguridad medioambiental	M-5-2	Seguridad física y ambiental	Bajo
Garantías	**Destinatarios**		
Disponibilidad e integridad	Todos los usuarios		

Desarrollo

Propósito

Prevenir los daños físicos de la ITT.

Exposición

Medidas generales (que aplican a la ITT aunque no se han definido explícitamente para la ITT).

Sobre salas de albergue de servidores:

- Las salas deberán de incorporar de diferentes sistemas que permitan mantener la infraestructura de la ITT bajo unas condiciones de operación óptimas. Además, estas medidas deberán de permitir la detección de eventos físicos que pudieran poner en peligro físicamente a la ITT:
  - Sistemas de detección de humos.
  - Sistemas automáticos de extinción de incendios.
  - Sistemas automáticos que permitan controlar la temperatura y humedad de la sala.
  - Falso techo y falso suelo técnico.
  - Sistemas de alimentación ininterrumpida.

Sobre armarios y otros contenedores de oficina:

- En el caso que se trate de armarios ubicados en zonas de oficina, éstos serán adecuados a la naturaleza del equipamiento albergado y atendiendo a características que permitan la protección frente amenazas externas como por ejemplo polvo, fuego y humedad.

Medida	Código	Objetivo	Alcance
Seguridad en equipos	M-5-3	Seguridad física y ambiental	Bajo
Garantías	**Destinatarios**		
Integridad, disponibilidad y confidencialidad	Administradores de sistemas		

Desarrollo

Propósito

Evitar la pérdida, daño, robo o compromiso de los equipos personales y la interrupción de las actividades de la Administración General de la CAPV y sus Organismos Autónomos en torno a la e-Administración.

Esta medida se orienta a los equipos personales que pueden estar fuera de Áreas Seguras tal como se expresa en M-5-1.

Exposición

- Se debe ubicar o proteger los activos de la ITT para evitar amenazas y peligros ambientales y accesos no autorizados. Se deben ubicar en lugares en los que se minimice el acceso innecesario.
- Se deben mantener correctamente los equipos para asegurar su disponibilidad e integridad.
- Se debe aplicar seguridad a los equipos que se encuentren fuera de los locales o áreas seguras de la Administración General de la CAPV y sus Organismos Autónomos teniendo en cuenta los diferentes riesgos que implica trabajar fuera de dichos locales. Sin importar la propiedad, el uso de cualquier equipo de procesamiento de la información fuera de los locales de la Administración General de la CAPV y sus Organismos Autónomos debe ser autorizado.
- El equipo de almacenamiento y procesamiento de la información incluye todas las formas de computadoras personales, agendas, teléfonos móviles, tarjetas inteligentes u otras formas que se utilicen para trabajar desde locales ajenos a los propios de la Administración.
- Los riesgos de seguridad como daño, robo o pérdida pueden variar sensiblemente entre unos locales (p.ej. Áreas Seguras) y otros (p.ej. un aeropuerto) y se debe tomar esto en cuenta para determinar los controles más apropiados.

Medida	Código	Objetivo	Alcance
Segregación de funciones	M-6-1	Gestión de comunicaciones y operaciones	Medio
Garantías	**Destinatarios**		
Integridad y confidencialidad	Desarrolladores, Administradores de sistemas		

Desarrollo:

Propósito

Asegurar que aquellas tareas que sean críticas para el servicio o la gestión del riesgo no recaerán sobre un único punto, reduciendo, de este modo, las oportunidades de acceso y manipulación indebida de información.

La segregación de funciones es un método de asignación de responsabilidades que permite reducir el riesgo de uso indebido, accidental o deliberado, de la información de cada una de los órganos competentes de la Administración General de la CAPV y sus Organismos Autónomos, separando la gestión o realización de ciertas operaciones sensibles. Mediante esta separación se asegura que aquellas tareas que sean críticas para el servicio o la gestión del riesgo no recaerán sobre un único punto, reduciendo, de este modo, las oportunidades de acceso y manipulación indebida de información.

Exposición

- A nivel de usuarios de la ITT, se realizará una asignación y segregación de privilegios para las transacciones en las que exista riesgo para las garantías de seguridad.
- A nivel de administradores de la ITT se realizará una asignación y segregación de privilegios para las operaciones en las que exista riesgo para las garantías de seguridad.
- Cabe mencionar que la realización y aprobación de transacciones y operaciones, petición y asignación de privilegios, implantación y seguimiento de controles son tareas que deberán permanecer segregadas.
- La asignación de operaciones en cada una de las áreas o departamentos se llevará a cabo según los criterios de segregación establecidos por las direcciones de cada una de las áreas o departamentos.
- En el caso de que, por motivos justificados, no sea posible realizar una segregación de funciones adecuada de cierta tarea o responsabilidad, se extremarán las medidas de seguimiento y supervisión de las mismas, con la finalidad de verificar su correcta realización y detectar posibles usos indebidos.
- Es responsabilidad de la dirección de cada órgano competente realizar un seguimiento periódico de las funciones y responsabilidades asignadas, con la finalidad de comprobar que se mantiene una adecuada segregación de funciones.
- Esta segregación de funciones se debe adoptar en los siguientes ámbitos:
  - Funcional
  - Desarrollo
  - Sistemas

Medida	Código	Objetivo	Alcance
Planificación de cambios	M-6-2	Gestión de comunicaciones y operaciones	Medio
Garantías	**Destinatarios**		
Integridad y confidencialidad	Desarrolladores, Administradores de sistemas		

Desarrollo:

Propósito

Mantener un control continuo de cambios realizados en el sistema, de forma que todos los cambios que se propongan a la ITT sean analizados para determinar su conveniencia para ser incorporados. Los cambios hay que planificarlos siempre para reducir el impacto sobre la prestación de los servicios afectados.

Exposición

Cambios en las aplicaciones y componentes de la ITT

- Los proyectos de desarrollo informático que se inicien en torno a la ITT se deben llevar a cabo considerando requisitos específicos de seguridad de la información durante todo el ciclo de desarrollo.
- En dicha construcción o desarrollo deberán tenerse en cuenta los siguientes principios:
  - En la fase de análisis y especificación de requerimientos de seguridad de la información se contemplarán los requisitos del dominio de seguridad.
  - Durante el desarrollo de aplicaciones a medida se deben tener en cuenta recomendaciones y buenas prácticas generalmente aceptadas de programación segura (validación de datos, documentación del código, almacenamiento y transmisión de información confidencial, control de errores, generación de registros y pistas de auditoría, acceso por parte de usuarios privilegiados o anónimos, empleo de mecanismos específicos de seguridad de la información, y otros que se consideren).
  - El desarrollo y las pruebas se realizarán usando ficheros y bases de datos de pruebas, tal como establecen las mejores prácticas sobre la protección de los datos de prueba del sistema.
  - Deberán establecerse los requisitos del control de cambios relativos a la seguridad de la información, que tendrán como finalidad evitar la pérdida de información o disponibilidad en el proceso de cambio.
  - Antes de implantar un software en producción, deberá ser revisado en busca de código malicioso que ponga en peligro la seguridad de la información de la Administración General de la CAPV y sus Organismos Autónomos.
- Para minimizar el riesgo por corrupción de los sistemas de información y comunicaciones se deben establecer controles en la implantación de cambios. Los cambios en el código de las aplicaciones pueden impactar negativamente en el entorno de producción. Para evitar estos impactos negativos se deben establecer reglas, que causen las mínimas interrupciones en las actividades del entorno de producción, sobre:
  - El acceso a los sistemas por parte de los programadores.
  - Los niveles de autorización.
  - La identificación de aplicaciones susceptibles de mejora.
  - El seguimiento de un control de las versiones.
  - Los criterios de actualización del software.
- Con anterioridad a la implantación de las mejoras en producción se debe de haber probado la

efectividad del software en el entorno de pruebas, comprobando que cumple con todas las medidas que se aplican en ámbitos como calidad del software, seguridad de la información especificadas por la normativa aplicable, etc. teniendo en especial cuidado en que los datos de prueba no pasen a producción.

- Tras esta operación, se debe actualizar la documentación de sistemas, archivándose y manteniendo un histórico de las versiones anteriores.

Cambios en el software de base de la ITT

- Se entenderá por software de base al conjunto de programas y utilidades necesarios para que funcionen las aplicaciones.
- Cuando los cambios realizados afecten al software de base, y muy en particular, al sistema operativo, éstos serán analizados, revisados y probados para asegurar que no impactan en la seguridad de la información.
- El proceso de cambios en el software de base deberá avisarse con la suficiente antelación para que los sistemas, y ocasionalmente las aplicaciones, puedan ser preparados previamente.
- Adicionalmente, ante cualquier cambio en los sistemas se deberán revisar los planes de continuidad de actividad, por si han resultado afectados.

Medida	Código	Objetivo	Alcance
Protección frente a código dañino	M-6-3	Gestión de comunicaciones y operaciones	Bajo
Garantías	**Destinatarios**		
Integridad, disponibilidad y confidencialidad	Administradores de sistemas		

Desarrollo

Propósito

Proteger la integridad del software y de la información ante amenazas concretas de tipo lógico (malware en general).

Exposición

- Todos los componentes de la ITT deberán tener una configuración segura (securización) antes de conectarse a cualquier tipo de red.
- La securización deberá ser especialmente restrictiva en los cortafuegos, equipos para garantizar la seguridad del entorno y en aquellos sistemas ubicados en segmentos de red expuestos a Internet u otras redes públicas.
- La implantación de la configuración segura será llevada a cabo por los responsables correspondientes.
- Las medidas de securización o parámetros de configuración segura, una vez definidas, analizadas y probadas, deberán incluirse en el plan de instalación de equipos.
- Los parámetros de configuración segura dependerán de la clasificación del activo en si mismo.
    - De la información que traten y de los grupos de usuarios que acceden. Los usuarios y grupos de usuarios que acceden al sistema, así como la clasificación de la información que dicho sistema alberga o trata, determinarán la asignación de privilegios en el sistema. Esta asignación se debe hacer según el principio de menor privilegio, limitando los permisos únicamente a los estrictamente necesarios para la operativa de los usuarios.
    - De los servicios de red que presten. Los servicios de red que el sistema debe proveer deberán ser identificados, deshabilitando el resto de servicios. Por defecto, todo servicio que no se necesite y autorice deberá ser deshabilitado, habilitándose posteriormente sólo aquellos que se soliciten expresamente. En este sentido, deberá ser tratada con especial atención la supresión de servicios de comunicaciones que puedan ser utilizados por usuarios que se conecten de forma remota.
- El proceso de securización incluirá la instalación y configuración del software necesario para la detección de intrusiones en el sistema, disponiendo de los correspondientes registros.
- También, deberán controlarse de una manera segura los accesos a los puertos de diagnóstico remoto, con el fin de evitar accesos no autorizados, debiéndose proteger con un mecanismo de seguridad adecuado y permaneciendo sólo accesibles a solicitud de las personas encargadas del mantenimiento del hardware o del software.
- Para la definición de la configuración de seguridad, los equipos técnicos encargados harán un seguimiento de las vulnerabilidades publicadas en listas abiertas de distribución o a partir de los boletines de los fabricantes. En cualquier caso, se analizará el impacto de la vulnerabilidad anunciada y el impacto de variar la configuración de seguridad. Se deberá ser diligente con las actualizaciones de seguridad publicadas por los fabricantes con el objetivo de evitar ataques “0-day” o de “día 0”.
- Se mantendrá documentación actualizada relativa a las configuraciones seguras de los sistemas. Esta documentación tendrá carácter confidencial.

Actividades

- Proceso de securización y gestión de parches y vulnerabilidades.

Medida	Código	Objetivo	Alcance
Seguridad en los servicios de red	M-6-4	Gestión de comunicaciones y operaciones	Bajo[++]
Garantías	**Destinatarios**		
Integridad, disponibilidad y confidencialidad	Administradores de sistemas		

Desarrollo

Propósito

Asegurar la protección de la información en las redes.

Exposición

- En todo contrato de redes se deben identificar e incluir las características de seguridad, niveles de servicio y requerimientos de todos los servicios de red, independientemente de que esta provisión sea interna o externa.
- Se debe determinar y monitorizar regularmente la capacidad del proveedor de servicio de red para manejar los servicios contratados de una manera segura, y se debe acordar el derecho de auditoría.
- Se deben identificar los acuerdos de seguridad necesarios para servicios particulares, como las características de seguridad, niveles de servicio y requerimientos de gestión. La Administración General de la CAPV y sus Organismos Autónomos debe asegurarse que los proveedores de servicio de red implementen estas medidas.
- Los servicios de red incluyen la provisión de conexiones, servicios de redes privadas, redes de valor agregado y soluciones de seguridad de red manejadas como firewalls y sistemas de detección de intrusiones.
- Se deben implantar controles de autenticación, codificación y conexión de red. La fortaleza de los controles a implementar se realizará en base a un análisis de riesgos previo.

Actividades

- Gestión de Acuerdos de Nivel de Servicio

Medida	Código	Objetivo	Alcance
Manipulación de los soportes	M-6-5	Gestión de comunicaciones y operaciones	Bajo[+]
Garantías	**Destinatarios**		
Integridad y confidencialidad	Todos los usuarios.		

Desarrollo

Propósito

Evitar la revelación, modificación o destrucción no autorizada de los activos de la organización (en este caso pueden ser tanto soportes electrónicos como no electrónicos –soporte papel–) durante su custodia y transporte, e implantar una política de borrado y destrucción segura de los mismos.

Exposición

- Estos soportes deberán ser protegidos contra accesos no autorizados, mal uso o corrupción durante su transporte. Por ejemplo, se puede realizar un envío en varias entregas y por rutas diferentes, utilizando un empaquetamiento seguro, tanto en lo que se refiere a factores ambientales (humedad, calor…) como humanos (contenedores cerrados con llave, entrega en mano…)
- La información contenida en soportes electrónicos deberá utilizar técnicas criptográficas, tal y como se establece en la medida M-8-2.
- Los soportes que contienen información confidencial, una vez finalizada su función, deben ser destruidos físicamente, borrados o sobre-escritos utilizando técnicas que hagan imposible recuperar la información original.

Medida	Código	Objetivo	Alcance
Copias de seguridad	M-6-6	Gestión de comunicaciones y operaciones	Medio

Garantías	Destinatarios
Integridad, disponibilidad, confidencialidad y conservación	Administradores de sistemas

Desarrollo

Propósito

Mantener la integridad y disponibilidad de la información y de los recursos de tratamiento de la misma a través de un sistema robusto de copias de seguridad.

Teniendo en cuenta que la información puede estar "*estructurada*" (en el caso de que la información resida en un sistema centralizado y la información esté organizada lógicamente en una base de datos y se acceda a esta información a través de la ITT) o no "*estructurada*" (en el caso de que la información no resida en un sistema centralizado sino que se encuentre disgregada en ficheros ofimáticos sin una organización única y clara; este tipo de información puede ser generada por la propia ITT o ser parte de los procesos de gestión con los ciudadanos que los procesos que soporte la ITT necesite).

Exposición

- Los encargados de la función de administración y operación de los sistemas deberán realizar copias de respaldo periódicas de toda la información contenida en sistemas de información ITT, para la cual se haya previsto un plan de salvaguarda. En dichas copias se considerará el respaldo de los datos, de los datos de configuración de los sistemas, del software, de los registros de eventos y pistas de auditoría y de la documentación necesaria para su posterior recuperación.
- No se contemplará la realización de copias de seguridad de los datos almacenados localmente en las estaciones de trabajo de los empleados.
- La periodicidad de realización de las copias de respaldo ha de ser directamente proporcional a la relevancia o sensibilidad de la información almacenada, a la frecuencia de su modificación o actualización y al riesgo de que el sistema falle o se corrompa, quedando establecida en el plan de salvaguarda siempre cumpliendo los requisitos que establece el Reglamento de la LOPD en este ámbito.
- El fallo o la no realización de la copia de seguridad será considerado y reportado como incidencia de seguridad.

Actividades identificadas en esta medida:

- Gestión de copias de seguridad

Medida	Código	Objetivo	Alcance
Canales de comunicación	M-6-7	Gestión de comunicaciones y operaciones	Bajo

Garantías	Destinatarios
Confidencialidad e integridad	Todos los usuarios

Desarrollo

Propósito

Establecer las medidas de seguridad en aquellos canales de comunicación telemáticos admitidos en la ley de Administración Electrónica pero que no forman parte de los mecanismos de seguridad que implementa la ITT.

Exposición

- La ITT dispone de su propio sistema de notificaciones más robusto y seguro que medios telemáticos clásicos (correo electrónico, fax, teléfono). Por este motivo, estos otros canales de comunicación se considerarán medios alternativos con los que se podrá iniciar trámites administrativos siempre y cuando exista la medida de seguridad que permita identificar de forma inequívoca al ciudadano que desea iniciar el trámite administrativo. El resto de notificaciones telemáticas u otros requerimientos se realizarán a través de la ITT.
- Dentro del ámbito de la ITT, el uso del teléfono será utilizado como método para iniciar trámites administrativos siempre y cuando se establezca un protocolo de control que permita la identificación clara del ciudadano.
- Dentro del ámbito de la ITT, el uso del correo electrónico será utilizado como método de comunicación interna entre funcionarios y como medio alternativo de comunicación informal con el ciudadano.
- Se prestará especial atención en no emplear el correo electrónico como medio de comunicación para enviar o recibir información crítica para la Administración.

Medida	Código	Objetivo	Alcance
Protección de contenidos en servicios y aplicaciones web	M-6-8	Gestión de comunicaciones y operaciones	Bajo
Garantías	**Destinatarios**		
Disponibilidad, confidencialidad e integridad	Administradores de sistemas		

Desarrollo:

Propósito

Proteger la información que esté disponible públicamente para que no sea modificada de forma no autorizada.

Exposición

- Con la finalidad de proteger la integridad de sus contenidos, los sistemas de acceso público de la ITT deberán tener instalados y activos mecanismos que permitan descubrir de forma automática si han sido modificados de forma no autorizada.
- Cuando se detecten modificaciones no autorizadas de los contenidos, estos sistemas deberán generar las alertas necesarias al personal encargado de la operativa de los sistemas de acceso público y permitir una rápida restauración de los contenidos originales, ya sea de forma manual o automática.
- En este caso, se deberá reportar una incidencia a la mayor brevedad posible para que se realice un análisis de la incidencia.

Medida	Código	Objetivo	Alcance
Planificación del sistema	M-6-9	Gestión de comunicaciones y operaciones	Medio[+]
Garantías	**Destinatarios**		
Integridad, disponibilidad y confidencialidad	Desarrolladores, Administradores de sistemas		

Desarrollo

Propósito

Minimizar el riesgo de fallos en los sistemas. Para lograrlo se fijan dos iniciativas: la gestión de las capacidades del sistema y el establecimiento de criterios formales para la aceptación de modificaciones o nuevos sistemas de información.

Exposición

- Se debe monitorizar, afinar el uso de los recursos y se deben realizar proyecciones de los requerimientos de capacidad futura para asegurar el desempeño deseado de la ITT.
- Se debe identificar los requerimientos de capacidad de cada actividad nueva y en proceso, así como planificar la afinación y monitoreo del sistema para asegurar y mejorar la disponibilidad y eficiencia de los mismos. Se debe prestar atención a aquellos recursos con largos tiempos de espera de abastecimiento.
- Se debe establecer, también, el criterio de aceptación de los sistemas de información nuevos, actualizaciones o versiones nuevas y se deben realizar pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación.
- Los responsables de los activos deben asegurar que los requerimientos y criterios de aceptación de los sistemas nuevos estén claramente definidos, aceptados, documentados y probados.
- Los sistemas de información nuevos, las actualizaciones y las versiones nuevas deben migrar a la producción después de obtener aceptación formal.
- La aceptación de un nuevo proceso puede incluir un proceso de certificación y acreditación formal para verificar que se hayan tratado apropiadamente los requerimientos de seguridad.

Medida	Código	Objetivo	Alcance
Supervisión	M-6-10	Gestión de comunicaciones y operaciones	Medio[+]
Garantías	**Destinatarios**		
Integridad y confidencialidad	Todos los usuarios.		

Desarrollo

Propósito

Detectar y reaccionar ante comportamientos sospechosos o inesperados, se establecerán sistemas de registro de actividades (logs) que almacenen los datos generados por las actividades de la ITT y sus usuarios. Estos sistemas de registro deberán permanecer activos siempre que dichos sistemas, redes, aplicaciones e identificadores de usuario se encuentren operativos.

Exposición

- Para cada activo, y dependiendo de su tipo, se definirán los mecanismos de registro y localización adecuados. Estos mecanismos deberán de incorporar la capacidad de seleccionar el nivel de detalle del registro generado.
- Las aplicaciones deberán generar registros de actividad que permitan de manera sencilla realizar seguimiento de operaciones y eventos. Los registros deberán ser almacenados de forma transparente.
- Los mecanismos de registro de eventos deberán generar una alerta si, por cualquier motivo, no es posible generar el registro.
- Debido a la información que aportan los registros de eventos sobre los sistemas, redes, aplicaciones y usuarios, el acceso a estos registros deberá quedar limitado a las personas autorizadas para su análisis.
- Los registros deberán protegerse de modificación o eliminación no autorizada. En el caso de transferencia de registros a través de redes de comunicación, ya sea para lectura remota o para enviar los registros a repositorios centrales, deberán protegerse frente a modificación o acceso no autorizado.
- Los registros se guardarán durante periodos predefinidos, que cómo mínimo serán los establecidos por la legislación vigente en cada momento.
- Los registros de eventos serán utilizados como pistas de auditoría en la función de revisión y control. En consecuencia, y con el fin de mantener una adecuada correlación entre registros generados por diferentes sistemas, los relojes de todos los sistemas deben estar sincronizados.
- Los registros de información (datos tributarios, administrativos, contables, o cualquier otra información relevante, imprescindible desde el punto de vista legal) que recojan la actividad de la Administración General de la CAPV y sus organismos autónomos deben ser almacenados y protegidos frente a pérdida, destrucción, alteración y falsificación, de manera que se cumpla con la legislación vigente.

Actividades

- Gestión de logs

Medida	Código	Objetivo	Alcance
Operaciones sobre activos físicos fuera de las áreas seguras	M-6-11	Gestión de comunicaciones y operaciones	Bajo
Garantías	**Destinatarios**		
Integridad y confidencialidad	Todos los usuarios		

Desarrollo:

Propósito

Evitar el uso indebido, deterioro o acceso no autorizado de los activos de la ITT que contengan información durante el transporte de los mismos fuera de las áreas seguras de la organización. Esta medida no aplica a los equipos personales (ver medida M-5-3).

Exposición

- Los equipos y soportes de datos de la ITT sacados de su lugar habitual de trabajo no se dejarán desatendidos en sitios públicos.
- Se cubrirán con un seguro adecuado los equipos sacados de su lugar de trabajo, y se tendrán en cuenta en el traslado las instrucciones proporcionadas por el fabricante para proteger los equipos.
- Se evitará, en la medida de lo posible, que el equipo contenga información sensible. Si es posible, la información debería de eliminarse de forma segura antes de salir fuera de las áreas seguras.

Medida	Código	Objetivo	Alcance
Proceso de autorización / Acceso de usuarios	M-7-1	Control de acceso	Bajo
Garantías	**Destinatarios**		
Autenticidad y confidencialidad	Todos los usuarios.		

Desarrollo

Propósito

Formalizar el proceso de autorización que establezca los controles necesarios para decidir si un objeto (persona, programa o dispositivo) tiene permiso para acceder a la ITT (autenticación) y con qué nivel de privilegio (autorización).

Exposición

- Se debe controlar el acceso a la información y los medios de procesamiento de la información sobre la base de requerimientos de seguridad.
- Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad para el acceso. Las reglas de control de acceso y los derechos para cada usuario o grupos de usuarios se deberían establecer claramente. Los controles de acceso deben ser tanto físicos como lógicos y estos deben ser considerados juntos.
- Se debe proporcionar a los empleados y externos un enunciado claro de los requerimientos que deben cumplir los controles de acceso. Las reglas de control de acceso deben ser respaldadas por procedimientos formales y responsabilidades claramente definidas.
- Se deben establecer procedimientos formales adecuados para controlar la asignación de los derechos de acceso a los sistemas y servicios de información dentro del ámbito de la ITT. Por tanto, debe existir un procedimiento formalizado para el registro y des-registro de usuario para otorgar y revocar el acceso a todos los sistemas y servicios de información así como controlar la asignación y uso de privilegios.
- Los procedimientos deben abarcar todas las etapas en el ciclo del acceso del usuario, desde el registro inicial de usuarios hasta la cancelación de los mismos. Cuando sea apropiado, se debe prestar atención especial a la necesidad de controlar la asignación de derechos de acceso privilegiados, lo que permite que los usuarios superen los controles del sistema.
- Se debe considerar la posibilidad de establecer roles de acceso para facilitar la gestión de usuarios. Los roles deben de estar basados en los requerimientos que resuman un número de derechos de acceso típicos para los usuarios.
- Se debe considerar incluir en los contratos del personal y de contratos de servicio cláusulas que especifiquen las sanciones si el personal o los agentes del servicio intentan un acceso no autorizado.
- El acceso de los usuarios y el personal de soporte a la información y las funciones del sistema de la aplicación debe limitarse en concordancia con la política de accesos definida.
- Para el empleado se plantea un proceso de autorización en base a función pública (rol básico). Para acceder al resto de aplicaciones que necesite se realizará la gestión en base a un acceso discrecional.
- Para externos, el acceso a los aplicativos y sistemas se basará en base a un acceso discrecional.

Actividades

- Gestión de identidades y accesos

Medida	Código	Objetivo	Alcance
Control de acceso	M-7-2	Control de acceso	Bajo
Garantías	**Destinatarios**		
Autenticidad y confidencialidad	Todos los usuarios.		

Desarrollo

Propósito

Establecer los controles específicos que se deben de implementar a la hora de llevar a cabo la autenticación y la autorización de los objetos (persona, programa o dispositivo) en la ITT.

Exposición

- **Identificación y autenticación de personas usuarias**
  - El acceso a la ITT de la Administración General de la CAPV y sus Organismos Autónomos se realizará utilizando un identificador de usuario debidamente autorizado.
  - El identificador de usuario deberá estar asignado a una persona física, teniendo carácter personal e intransferible.
  - Asociado a cada identificador de usuario se conservarán en el sistema los datos que, como mínimo, permitan relacionar unívocamente el identificador con la persona usuaria, de forma que a cada persona usuaria se le pueda responsabilizar de las actividades realizadas con su identificador de usuario.
  - El uso de identificadores y contraseñas para el acceso a los sistemas de información y comunicaciones, así como los procedimientos de verificación asociados, deben asegurar la identidad de los empleados, permitiendo asignar privilegios de acceso personalizados.
- **Usuarios temporales**
  - Los usuarios que no sean plantilla fija de la Administración General de la CAPV y de sus Organismos Autónomos deben recibir identificadores temporales que sigan los mismos procesos de aprobación que para los nuevos empleados. Los derechos de acceso de estos usuarios deben otorgarse sólo por el periodo de tiempo necesario.
- **Usuarios genéricos**
  - No está permitida la creación o utilización de usuarios genéricos.
  - Todos los usuarios deberán tener asignado un responsable unívoco bien identificado.
  - Asimismo, salvo en situaciones justificadas por el desempeño de las funciones, cada persona física tendrá asociado un único identificador de usuario. Como excepción, una persona podrá disponer de más de un identificador de usuario en caso que los privilegios asignados a cada uno de los identificadores sean distintos y no sea técnicamente posible recogerlos todos en un único identificador de usuario, o no sea recomendable, por motivos de seguridad, mantener todos los privilegios en un único identificador.
  - Las personas usuarias dispondrán de una única identificación para todos los sistemas, permitiendo, gracias a su identificador personal, determinar las operaciones realizadas por cada una de ellas en los distintos sistemas.
- **Bloqueo de identificadores de acceso**
  - Con el fin de evitar el acceso no autorizado, el proceso de identificación y autenticación de usuarios mediante la introducción del identificador de usuario y contraseña deberá estar dotado de controles para el bloqueo automático del usuario y su inhabilitación temporal, en los siguientes casos:
    - Por sobrepasar un número máximo de intentos. Si se introduce de forma incorrecta el identificador de usuario, o la contraseña de acceso, de forma reiterada un número prefijado de veces.

- Por inactividad del usuario en el sistema. Si no se accede al sistema en un plazo superior a un número de días naturales prefijado.

- En estas situaciones, o cualquier otra que origine un bloqueo del identificador de usuario, la persona deberá solicitar, por los procedimientos establecidos, la rehabilitación de su perfil de usuario y el correspondiente desbloqueo del identificador.
- Las cuentas de usuarios administradores no se bloquearán, con el objetivo de evitar ataques de denegación de servicio a dichos usuarios. En su lugar, siempre que sea técnicamente posible, se deberán establecer los controles compensatorios adecuados para monitorizar intentos fallidos de inicio de sesión con claves de usuario que tengan asignado perfil administrador.

Medida	Código	Objetivo	Alcance
Acceso a red	M-7-3	Control de acceso	Bajo
Garantías	**Destinatarios**		
Autenticidad, confidencialidad y trazabilidad	Todos los usuarios		

Desarrollo

Propósito

Prevenir el acceso no autorizado a los servicios de red sean éstos internos o externos.

Los accesos a la red corporativa de la Administración General de la CAPV y de sus Organismos Autónomos, cuyo origen sea externo conllevan un elevado nivel de riesgo (apertura de la red corporativa a redes y sistemas externos no conocidos y no controlados; posibilidad de que las redes o sistemas controlados tengan a su vez otras conexiones; etc.).

Esta medida recoge como servicios de acceso remoto permitidos aquellos que respondan a necesidades de actividad, mantenimiento y soporte.

Exposición

- Habrá que establecer mecanismos para tratar convenientemente la información transmitida, los sistemas y recursos accedidos, la identidad de las personas que realizan dichos accesos y las posibles implicaciones que el acceso en global conlleva.
- Los servicios de acceso remoto deberán de disponer de mecanismos de autenticación basados, cuando menos, en el par usuario-contraseña (siempre a través de canal cifrado) o criptografía de clave pública. Al mismo tiempo, dependiendo de la criticidad de la información, la comunicación deberá estar cifrada. De manera imprescindible, la contraseña deberá transmitirse siempre de forma ininteligible.
- Los usuarios con privilegios de acceso remoto deberán asegurar que su equipo cuando está conectado de forma remota a la red corporativa de la Administración General de la CAPV y de sus Organismos Autónomos, no estará simultáneamente conectado a ninguna otra red.
- Es responsabilidad de los empleados con privilegios de acceso remoto asegurar que éste no es usado por empleados no autorizados o externos a la Administración. Los empleados con posibilidad de acceder remotamente a la red interna deberán recordar constantemente que las conexiones remotas entre su equipo y la Administración son extensiones literales de la red corporativa, y que proporcionan una vía de acceso potencial hacia información confidencial. Los empleados deberán tomar todas las medidas posibles y razonables para proteger los activos de la Administración General de la CAPV y sus Organismos Autónomos.
- Por ello, estará prohibido transmitir identificadores de usuario, contraseñas o credenciales, configuraciones de la red interiores o direcciones a través de Internet. En caso de necesidad esta información se enviará cifrada.
- Las conexiones que se llevan a cabo entre redes de la Administración General de la CAPV y sus Organismos Autónomos deben permitir únicamente el tráfico estrictamente necesario y autorizado. Para ello se deben utilizar elementos de filtrado (como cortafuegos) que definan el perímetro de cada red conforme a las normas de interoperabilidad establecidas.
- El criterio de separación de redes mediante perímetros persigue la segmentación en redes físicamente independientes, agrupando componentes con requisitos o características similares desde el punto de vista de seguridad de la información.
- Los flujos de tráfico entre redes situadas en distintos perímetros de seguridad se basarán en los tipos de tráfico permitidos y no permitidos entre ellas.
- Con el fin de ocultar los esquemas internos de direccionamiento IP, además de para solucionar problemas derivados de conflictos en planes de direccionamiento se debe poder hacer uso de mecanismos de traducción de direcciones (p. ej. NAT).

Medida	Código	Objetivo	Alcance
Responsabilidades de usuario	M-7-4	Control de acceso	Bajo
Garantías	**Destinatarios**		
Autenticidad y confidencialidad	Funcionarios		

Desarrollo

Propósito

Prevenir el acceso de usuarios no autorizados y, por tanto, evitar el robo o compromiso de información no divulgable o especialmente protegida por ley.

Los usuarios deben de ser conscientes y sensibles respecto a su nivel de responsabilidad para mantener un control de acceso efectivo. Especialmente respecto al uso de contraseñas.

Exposición

- Todos los empleados de la Administración General de la CAPV y sus Organismos Autónomos seguirán unas reglas de limpieza de escritorio y pantalla, de modo que los dispositivos de almacenamiento, documentación e información queden protegidos cuando el empleado abandone su puesto de trabajo.
- Estas reglas serán conocidas por todos los empleados de la Administración como parte de su formación y concienciación en seguridad de la información.
- En ellas se especificarán las siguientes directrices:
  - La documentación, informes y medios informáticos tales como cintas o discos, deberán guardarse bajo llave, especialmente fuera del horario de trabajo. La información sensible o crítica deberá ser guardada en un sitio seguro, bajo llave, cuando no se requiera, especialmente cuando la oficina esté vacía.
  - Las estaciones de trabajo, terminales e impresoras deberán disponer de autenticación, llave u otro tipo de mecanismo de control de acceso y bloqueo automático en caso de permanecer desatendidos.
  - Los buzones de correo no deberán permanecer desatendidos si no están protegidos.
  - En los entornos donde se maneje información confidencial cuyo soporte físico sea el papel, se deberán proteger las fotocopiadoras del uso no autorizado fuera del horario de trabajo.
  - La información sensible o clasificada impresa deberá recogerse inmediatamente de las impresoras.

Medida	Código	Objetivo	Alcance
Requisitos de seguridad	M-8-1	Adquisición, desarrollo y mantenimiento de los sistemas de información	Bajo
Garantías	**Destinatarios**		
Integridad y confidencialidad	Desarrolladores, Administradores de sistemas		

Desarrollo

Propósito

Asegurar que los requerimientos/medidas de seguridad son una parte integrada de la ITT.

Exposición

- En las declaraciones de los requisitos de servicio para nuevos sistemas de información o modificación de los sistemas existentes se deben de especificar requisitos concretos de seguridad.
- Los enunciados de los requerimientos comerciales para los sistemas de información nuevos, o las mejoras a los sistemas de información existentes de la ITT, deben especificar los requerimientos de controles de seguridad.
- Dichos requerimientos y controles deben reflejar el valor comercial de los activos de información involucrados y el daño comercial potencial que podría resultar de un fallo o ausencia de seguridad.
- Estos requerimientos deben ser integrados en las primeras etapas de los proyectos de sistemas de la información. Los controles introducidos en esta etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implantación.
- Si se considera apropiado, la gerencia puede desear hacer uso de productos evaluados y certificados independientemente. Se puede encontrar mayor información sobre el criterio de evaluación de los productos de seguridad de TI en ISO/IEC 15408.

Actividades

- Análisis de requisitos de seguridad

Medida	Código	Objetivo	Alcance
Criptografía	M-8-2	Adquisición, desarrollo y mantenimiento de los sistemas de información	Medio

Garantías	Destinatarios
Autenticidad, integridad y confidencialidad	Desarrolladores, Administradores de sistemas

Desarrollo

Propósito

Proteger la información desde un punto de vista de confidencialidad, autenticidad e integridad, utilizando técnicas criptográficas. Aún así, no hay que minusvalorar la gestión de claves que usen los diferentes sistemas criptográficos.

Exposición

Aquellos sistemas de información que precisen gestionar claves criptográficas, deberán disponer del software necesario para gestionarlas y cifrar la información, debiendo permitir:

- **Generación de claves**.
- **Distribución de claves empleando un canal seguro**.
- **Activación de claves**.
- **Almacenamiento y acceso a las claves**. Las claves deberán estar fuertemente protegidas físicamente y sólo permitido el acceso a las mismas con las más estrictas autorizaciones con el fin de preservar su confidencialidad.
- **Cambio o actualización de claves**. En caso de cambio, se deberá aplicar un proceso de re-distribución de la nueva clave y, en su caso, abandono y/o destrucción de la anterior.
- **Compromiso de las claves**. Se deberán establecer procedimientos y responsabilidades para la notificación del compromiso de las claves, así como de las medidas a tomar en aquellas situaciones que pongan en peligro la confidencialidad de las mismas.
- **Recuperación de claves**. En caso de pérdida o deterioro de claves criptográficas, se deberán establecer procedimientos, responsabilidades y mecanismos para la recuperación de claves especificando las condiciones necesarias para proceder a la recuperación, de forma que se garantice el acceso a la información que haya sido cifrada con dichas claves.
- **Archivado de claves** (fideicomiso de claves). En los casos en que los requisitos de confidencialidad sean elevados, se deberán emplear técnicas de división de claves en diferentes localizaciones o a diferentes figuras, de modo que se asegure que la custodia de las mismas se realiza sólo en condiciones de máxima seguridad.
- **Destrucción de claves**. Se deberán establecer procedimientos y responsabilidades para la destrucción de claves, donde se asegure que no existen datos que hayan sido cifrados usando dichas claves.
- **Registro de las operaciones relacionadas con la gestión de claves**. Se deberán mantener registros de las actividades realizadas, registrando, al menos:
    - Los destinatarios de las claves simétricas.
    - Los responsables de cada actividad.
    - La fecha de realización de cada una de las actividades.
- La selección de los algoritmos a utilizar deberá considerar la legislación vigente relativa al uso de mecanismos de cifrado. Otros aspectos a considerar en la selección de algoritmos de cifrado deberán ser la fortaleza y la eficiencia del algoritmo, así como el tipo de cifrado, simétrico o

asimétrico.

- La longitud de las claves de cifrado será acorde al periodo de tiempo durante el cual se pretende asegurar la confidencialidad de los datos que se van a cifrar.
- Las claves de cifrado se considerarán información secreta y, como tal, su acceso deberá estar limitado al propietario de las mismas. Las claves de cifrado se deberán generar por medios que garanticen su fortaleza. Todo programa o archivo que contenga fórmulas, algoritmos u otras especificaciones que se utilicen para la generación de claves debe estar controlado con las máximas medidas de seguridad.
- Las claves de cifrado deben ser ininteligibles y no se deben incluir dentro de los programas software. Los ordenadores y sistemas de comunicación deben tener implementados controles que impidan la recuperación de las claves almacenadas.
- Cuando sea necesario asegurar la disponibilidad de la información cifrada se utilizarán sistemas de cifrado que dispongan de recuperación de claves.
- Para la selección de soluciones de cifrado adecuadas a las necesidades de las aplicaciones y la información se establecerán las siguientes especificaciones de seguridad:
  - Se identificará la normativa de carácter legal o regulatoria referente a controles de cifrado.
  - Para cada caso se deberá determinar el algoritmo de cifrado que se empleará para preservar la confidencialidad de la información, realizando un análisis cuyo resultado especifique al menos los siguientes requerimientos de seguridad:

Utilización del algoritmo o solución

- Nivel donde se procederá al cifrado de la información:
  - En transmisión, pudiendo cifrarse dentro de la aplicación o en la transmisión.
  - En almacenamiento, pudiendo cifrarse la base de datos o sistema de ficheros.
- Escalabilidad de la solución, considerando las necesidades de expansión futura, en particular el sistema de intercambio de claves deberá ser adecuado, teniendo en cuenta que las soluciones basadas en secreto compartido no escalan de forma adecuada.
- Funcionalidades adicionales soportadas por la solución escogida, tales como:
  - Soporte para diferentes métodos de intercambio de claves.
  - Número de algoritmos de cifrado que soporta para intercambio con otros sistemas.
- Método de cifrado soportado por la solución:
  - Cifrado por hardware
  - Cifrado por software
- Posibilidades de ampliación futura de la solución, incorporando nuevas operaciones criptográficas.
- En los sistemas de información y comunicaciones de la Administración General de la CAPV y sus Organismos Autónomos se usará la técnica de firma electrónica cuando sea necesario garantizar el no repudio del mensaje o transacción mediante la autenticidad de origen y la integridad de la información.
- La utilización de la técnica de firma, en los términos establecidos por la legislación vigente, supone el uso de certificados digitales emitidos por una autoridad de certificación reconocida.

Medida	Código	Objetivo	Alcance
Aceptación y puesta en servicio	M-8-3	Adquisición, desarrollo y mantenimiento de los sistemas de información	Bajo
Garantías	**Destinatarios**		
Integridad y disponibilidad	Desarrolladores, Administradores de sistemas		

Desarrollo

Propósito

Minimizar el riesgo de corrupción de software durante el proceso de implantación de software en los entorno de producción de la ITT. Este proceso debe estar totalmente controlado. Esta medida complementa la medida M-6-2.

Exposición

- La actualización de las librerías de programas sólo se debe realizar tras haber concluido con éxito las correspondientes pruebas y tras obtener la autorización del usuario final.
- Las actualizaciones serán realizadas por técnicos especialistas y quedarán registradas como pistas de auditoría.
- Será necesaria una autorización por escrito del responsable del activo.
- Se mantendrá exclusivamente el código ejecutable.
- El código ejecutable no será pasado al entorno de producción hasta que no se hayan realizado pruebas y el resultado haya sido aceptado.
- Las características o funcionalidades que sean innecesarias en el entorno de producción se identificarán y desactivarán en el momento de la instalación del softwarę.
- Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías del entorno de pruebas a las librerías del entorno de producción, sin que previamente sean compilados por el área asignada.
- Las versiones anteriores se mantendrán como medida de seguridad. Se realizarán las copias de seguridad necesarias antes del pase al entorno de producción.
- Para cada aplicación, deberán existir procedimientos de gestión de errores que permitan la trazabilidad de éstos.
- Antes de realizar modificaciones del software, deberán revisarse los contratos de mantenimiento con los externos del mismo, ya que muchos de ellos no permiten que el cliente las realice sin su autorización.
- Si existe la posibilidad, para el paso desde los entornos de desarrollo o pruebas al entorno de producción, se utilizarán herramientas automáticas que realicen un control de versiones de software y permitan restaurar los sistemas en caso de fallo.
- Como medida de precaución ante posibles desastres se debe mantener un registro de todas las actualizaciones de las librerías de programas y se deben almacenar durante un tiempo las versiones anteriores.
- Las mismas precauciones se deben aplicar al software adquirido a terceros, en este caso se deben considerar las indicaciones de soporte del proveedor.

Medida	Código	Objetivo	Alcance
Gestión de incidencias	M-9-1	Gestión de incidentes de seguridad de la información	Medio
Garantías	**Destinatarios**		
Integridad, disponibilidad y confidencialidad	Todos los usuarios		

Desarrollo

Propósito

Garantizar que los eventos y debilidades de la seguridad de la información asociados con la ITT sean comunicados de una manera que permita que se realice una acción correctiva oportuna, se establecerán procedimientos formales de reporte y de escalado de un evento.

Exposición

- Todos los empleados y externos relacionados con la Administración General de la CAPV y sus Organismos Autónomos deben estar avisados de los procedimientos para el reporte de los diferentes tipos de eventos y debilidades que podrían tener un impacto en la seguridad de los activos. Se les deberá requerir que reporten cualquier evento y debilidad de la seguridad de la información lo más rápidamente posible según el procedimiento de contacto definido.
- El procedimiento de reporte de incidencias deberá incluir:
  - Procesos de notificación adecuados para asegurar que aquellos que reportan eventos en la seguridad de la información sean notificados de los resultados después de haber tratado y terminado con el problema.
  - Formatos de reporte los eventos en la seguridad de la información para respaldar la acción de reporte, y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento en la seguridad de la información.
  - Indicaciones para actuar de forma correcta en caso de ocurrencia de un evento de seguridad:
    - Anotar todos los detalles importantes inmediatamente (por ejemplo, el tipo de no-cumplimiento o violación, mal funcionamiento actual, mensajes en la pantalla, conducta extraña);
    - No llevar a cabo ninguna acción por cuenta propia, sino reportar inmediatamente al punto de contacto;
    - Referencia a un proceso disciplinario formal establecido para tratar con los usuarios empleados, o externos que cometen violaciones de seguridad.
- Para garantizar una gestión de incidentes efectiva, se establecerán las responsabilidades y procedimientos necesarios para manejar de manera adecuada los eventos y debilidades en la seguridad de la información una vez que han sido reportados.
- Se aplicará un proceso de mejora continuo para la respuesta, monitorización, evaluación y la gestión general de los incidentes en la seguridad de la información. Cuando se requieran evidencias, estas se recogerán cumpliendo con los requerimientos legales.
- Además de reportar los eventos y debilidades en la seguridad de la información, se utilizará la monitorización de los sistemas, alertas y vulnerabilidades para detectar los incidentes en la seguridad de la información. Se tendrá en cuenta:
  - Deben existir diferentes procedimientos para manejar los diferentes tipos de incidentes de seguridad.
  - Los procedimientos incluirán:
    - Análisis de la causa del incidente.

- Contención.
- Implementación de la acción correctiva.
- Comunicaciones a los afectados.
- Reporte de la acción a los interlocutores apropiados.

- Se recolectarán y asegurarán los rastros de auditoría y evidencias similares, para:
  - Realizar el análisis interno del problema.
  - Usar como evidencia forense en relación a una violación potencial del contrato o el requerimiento regulador o en el caso de una acción legal civil o criminal.
  - Negociar para la compensación de los proveedores del software o del servicio afectado.
- Se controlarán las acciones para recuperar el funcionamiento normal de los sistemas, asegurando que:
  - Sólo el personal claramente identificado y autorizado tendrá acceso a los sistemas y los datos.
  - Se documentan en detalle todas las acciones de emergencia realizadas;
  - Las acciones de emergencia se reporta a la gerencia y es revisada de una manera adecuada.
  - La integridad de los sistemas será reestablecida con la demora mínima.

- Se acordarán con la dirección los objetivos para la gestión de incidentes de seguridad de la información y se garantizará que los responsables e implicados en la resolución de las mismas entiendan las prioridades de la organización para el manejo de los incidentes en la seguridad de la información.

Actividades

- Gestión de incidentes de seguridad

Medida	Código	Objetivo	Alcance
Medios alternativos	M-10-1	Gestión de la continuidad del servicio	Alto
Garantías	**Destinatarios**		
Integridad, disponibilidad y conservación	Administradores de sistemas		

Desarrollo

Propósito

Establecer un entorno de trabajo único/común que permita implementar estrategias de continuidad de servicio.

Exposición

- Teniendo en cuenta que la información es uno de los activos más importantes de la Administración General de la CAPV y de sus Organismos Autónomos es necesario reducir el riesgo que supone la pérdida total o parcial de la misma dentro del ámbito de la ITT.
- Para ello, la información depositada en servidores centrales, servidores de redes, servicios de comunicación y, en general, cualquier información relevante para la operativa de la ITT debe estar sujeta a copias de respaldo periódicas que permitan su recuperación ante una pérdida imprevista.
- Las condiciones de almacenamiento deberán garantizar que no se producen deterioros en los soportes por causas ambientales, tales como temperaturas extremas, campos magnéticos, humedad, fuego, polvo, etcétera. Se debe llevar un control del estado de dichos soportes con el fin de prevenir su pérdida de calidad por envejecimiento y reutilización.
- Asimismo, deberá dotarse de mecanismos de control de acceso físico para el acceso a dichos soportes, pudiendo acceder a ellos únicamente el personal autorizado.

Actividades

- Gestión de la continuidad del servicio

Medida	Código	Objetivo	Alcance
Continuidad de servicio	M-10-2	Gestión de la continuidad del servicio	Medio
Garantías	**Destinatarios**		
Integridad, disponibilidad y conservación	Administradores de sistemas.		

Desarrollo

Propósito

Responder ante posibles interrupciones de actividad y proteger los activos de la Administración ante fallos de la ITT. Se deberá implementar un proceso de gestión de la continuidad del servicio para minimizar el impacto sobre la organización y recuperarse de la pérdida de activos hasta un nivel aceptable a través de una combinación de controles preventivos y de recuperación.

Exposición

- Este proceso debiera identificar los servicios críticos e integrar los requerimientos de gestión de la seguridad de la información de la continuidad del servicio con otros requerimientos de continuidad relacionados con aspectos como operaciones, personal, materiales, transporte y medios. Este proceso reunirá los siguientes elementos clave:
    - Entendimiento de los riesgos dentro de la e-Administración a los que la Administración General de la CAPV y sus Organismos Autónomos en términos de probabilidad e impacto en el tiempo, incluyendo la identificación y priorización de los servicios críticos.
    - Identificación de los activos involucrados en los diferentes servicios.
    - Entender el impacto que tendrían sobre el servicio la ocurrencia de un incidente de seguridad de la ITT.
    - Se considerará la compra de seguros como parte del proceso de continuidad de servicio.
    - De forma regular y ante cambios en el servicio se actualizarán y probarán los planes de continuidad, aplicando las medidas de mejora necesarias.
    - Se garantizará la seguridad del personal y la protección de los medios de procesado de información.
    - Se incorporará la continuidad del servicio a los procesos y se asignarán las responsabilidades apropiadas.
- Las consecuencias de los desastres, fallos en la seguridad, pérdida del servicio y la disponibilidad del servicio deben estar sujetas a un análisis del impacto en la actividad que se desarrolla. Se debieran desarrollar e implementar planes para la continuidad del servicio para asegurar la reanudación de las actividades esenciales.
- La gestión de la continuidad del servicio debiera incluir controles para identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, debiera limitar las consecuencias de incidentes dañinos y asegurar que esté disponible la información necesaria para el servicio que se presta.

Medida	Código	Objetivo	Alcance
Planes de continuidad de servicio que incluyan seguridad de la información	M-10-3	Gestión de la continuidad del servicio	Alto
Garantías	**Destinatarios**		
Integridad, disponibilidad y conservación	Administradores de sistemas		

Desarrollo

Propósito

Asegurar la vuelta a la normalidad del servicio de la ITT en previsión de posibles interrupciones o malfuncionamientos que provoquen la degradación de la capacidad de servicio de la misma. Para ello, se abordará la preparación, actualización periódica y prueba regular de Planes de Recuperación de Servicio.

Exposición

- Se deberá mantener Planes de Continuidad de Servicio que permitan la recuperación de sus servicios ante cualquier contingencia que los afecte.
- Los Planes de Continuidad de Servicio deben permanecer documentados, probados y actualizados, de tal manera que sean de conocimiento general y fácilmente aplicables en caso de desastre o contingencia.
- Estos planes deben contemplar, como mínimo, los riesgos más probables que puedan afectar a la continuidad de los procesos de la Administración General de la CAPV y sus Organismos Autónomos, permitir que los recursos previstos para superar la contingencia se encuentren disponibles y aseguren la continuidad de dichos procesos en el tiempo máximo establecido en cada uno de ellos.

Medida	Código	Objetivo	Alcance
Pruebas periódicas	M-10-4	Gestión de la continuidad del servicio	Alto
Garantías	**Destinatarios**		
Integridad, disponibilidad y conservación	Administradores de sistemas		

Desarrollo

Propósito

Probar los planes de continuidad de servicio con el fin de verificar que siguen siendo efectivos o adaptarlos en el caso de que los resultados de las pruebas no sean los adecuados.

Exposición

- Se elaborará un plan de pruebas para cada Plan de Continuidad de Servicio, que indicará cómo y cuándo será probado cada elemento del mismo. Dicho plan de pruebas incluirá simulaciones de distintos escenarios de activación, pruebas técnicas de recuperación, pruebas de recuperación en lugares alternativos, y cualesquiera otros ensayos.
- Los Planes de Continuidad de Servicio serán revisados periódicamente, para adaptarlos a los posibles cambios acaecidos. Asimismo, las responsabilidades de cada una de las personas involucradas en el plan serán actualizadas durante las revisiones periódicas.
- Además, y con carácter urgente, los planes de continuidad de la actividad se deberán actualizar si se producen:
    - Cambios de personal con responsabilidades asignadas en el plan.
    - Cambios en la estrategia de actividad.
    - Cambios de legislación.
    - Cambios en los recursos.
    - Cambios en las localizaciones.
    - Cambio en los contratos con externos.
- Se asignarán responsabilidades para la revisión, periódica o urgente, de cada Plan de Continuidad de Servicio, de manera que todos los cambios detectados y que no estuviesen reflejados hasta ese instante en dichos planes, deberán quedar actualizados de manera inmediata, tras el pertinente estudio.

Medida	Código	Objetivo	Alcance
Cumplimiento legal	M-11-1	Cumplimiento	Bajo
Garantías	**Destinatarios**		
Autenticidad, integridad, disponibilidad, confidencialidad y conservación	Todos los usuarios		

Desarrollo

Propósito

Detectar y evitar posibles brechas o problemas que pudieran estar presentes en la organización a nivel de seguridad relativa al entorno legislativo.

Exposición

- Es responsabilidad de la Administración General de la CAPV y sus Organismos Autónomos conocer en todo momento la normativa aplicable a la información y las comunicaciones de la ITT y mantener documentado el ámbito de aplicación de dicha normativa, el periodo de implantación de las medidas exigidas, y los procesos de revisión e inspección establecidos.
- En particular, se debe considerar la normativa relativa a los siguientes puntos:
  - Tratamiento de datos de carácter personal.
  - Privacidad de la información.
  - Contratos con externos.
  - Seguridad personal.
  - Derechos de propiedad intelectual.
  - Seguridad física y ambiental.
  - Infraestructura de los sistemas.
  - Acciones legales por negligencia o incumplimiento de contrato.
  - Recolección de pruebas ante delitos informáticos.
  - Auditoría de sistemas.
  - Monitorización de la información y derechos de los usuarios.
  - Uso de firma electrónica y algoritmos de cifrado.
  - Servicios telemáticos en la Sociedad de la Información.
- Asimismo, es responsabilidad de la DIT la actualización del Manual de Seguridad.
- Con la finalidad de proteger de forma adecuada la información de carácter personal tratada en la Administración General de la CAPV y sus Organismos Autónomos se tendrán en cuenta todas las normas recogidas en el presente Manual de Seguridad.

Actividades

- Gestión de auditorías

Medida	Código	Objetivo	Alcance
Cumplimiento técnico	M-11-2	Cumplimiento	Alto
Garantías	**Destinatarios**		
Autenticidad, integridad, disponibilidad, confidencialidad y conservación	Todos los usuarios		

Desarrollo:

Propósito

Detectar y evitar posibles brechas o problemas que pudieran estar presentes en la organización a nivel de seguridad relativa al entorno técnico.

Exposición

- La seguridad de la ITT se debe revisar regularmente.
  - Estas revisiones deben realizarse en base a las medidas de seguridad que apliquen a la ITT deben ser auditados en cumplimiento con los estándares de implementación de seguridad aplicables y los controles de seguridad documentados.
  - Los responsables (de los activos de la ITT) deben revisar regularmente el cumplimiento del procesamiento de la información dentro de su área de responsabilidad con las políticas y medidas de seguridad apropiadas, y cualquier otro requerimiento de seguridad.
  - Si se encuentra cualquier incumplimiento como resultado de la revisión, los responsables deben actuar para determinar cual es la causa y establecer una acción correctiva.
  - Estas revisiones y acciones deben quedar registradas.
  - El chequeo del cumplimiento técnico debe ser realizado por una persona con competencia (p.e. ingeniero de sistemas) y autorizado explícitamente para realizar dicha labor.

Medida	Código	Objetivo	Alcance
Análisis de riesgos	M-12-1	Gestión de la seguridad	Medio
Garantías	**Destinatarios**		
Todas las garantías de seguridad	Funcionarios		

Desarrollo

Propósito

Obligar a utilizar como herramienta de trabajo el análisis de riesgos en aquellas áreas de seguridad en las que sea necesario su uso.

Exposición

- La evaluación del riesgo debe incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo).
- Las evaluaciones del riesgo deben identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la Administración. Los resultados deben guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la ITT y para implementar las medidas de seguridad seleccionadas para protegerse contra estos riesgos.
- Las medidas de seguridad en las que es necesario realizar un análisis de riesgo son:
    - M-2-1
    - M-5-1
    - M-5-3
    - M-6-2
    - M-6-3
    - M-10-2
    - M-10-3

Medida	Código	Objetivo	Alcance
Mejora continua	M-12-2	Gestión de la seguridad	Medio
Garantías	**Destinatarios**		
Todas las garantías de seguridad	Funcionarios		

Desarrollo

Propósito

Establecer un proceso de mejora continua con el fin de mantener un sistema formal, que permita incrementar el nivel de madurez de la organización, en general, desde el punto de vista de la seguridad.

Exposición

- Se debe implementar un procedimiento para garantizar la mejora continua en el ámbito de la seguridad de la ITT. Para cumplir con este objetivo se necesita disponer de la información necesaria para responder preguntas sobre la eficiencia, eficacia, nivel de madurez o nivel de calidad del sistema de seguridad.
- Para ello se pueden utilizar métricas e indicadores que están reflejados en la ISO 27001 que contempla como uno de sus requisitos la necesidad de medir la eficacia de las medidas de seguridad para verificar el cumplimiento de los requisitos de seguridad.
- Una vez conocido el estado en que se encuentra en materia de seguridad se estará en disposición de tomar las decisiones oportunas en el momento idóneo gestionando de forma proactiva (antes que se produzcan situaciones y/o escenarios no deseados) la seguridad de la ITT.

Actividades

- Administración del Sistema de Gestión de la Seguridad.

5. Glosario

Acceso remoto: Acceso a la red interna a través de la red telefónica conmutada u otra red de acceso público.

Activo: Cualquier cosa que tenga valor para la organización. Más concretamente, recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Acuerdos de Nivel de Servicio (ANS): Ver definición de SLA (Service Level Agreement).

Amenaza: Cualquier circunstancia o evento capaz de causar daño a un sistema en la forma de denegación de servicio o destrucción, revelación no autorizada o modificación de datos.

Análisis de riesgos: Evaluación del posible impacto y probabilidad de materialización de las amenazas de seguridad a las que se encuentra expuesta una Organización. La finalidad es poder diseñar e implantar los controles de seguridad necesarios, establecer prioridades de implantación y reducir los riesgos existentes.

Antivirus: Programas informáticos que permiten analizar memoria, unidades de disco, mensajes o transmisiones en busca de virus. Una vez el antivirus ha detectado alguno de ellos, informa al usuario procediendo inmediatamente y de forma automática a desinfectar los ficheros, directorios, o discos que hayan sido víctimas del virus.

Ataques "zero-day" / "0 day" / "de día cero": Amenaza informatica que aprovecha vulnerabilidades de sistemas o aplicaciones que no disponen de una solución o parche conocido.

Auditoría de seguridad: Procedimiento usado para verificar que se están llevando a cabo controles en un sistema de información y que éstos son adecuados para los objetivos que se persiguen. Incluye el análisis de las actividades para detectar intrusiones o abusos dentro del sistema informático.

Autenticación: Proceso utilizado para confirmar la identidad y autenticidad de una persona ante un sistema o probar la integridad de información específica. En el caso de personas, el proceso de autenticación puede usar uno de los tres métodos siguientes:

- Algo que el usuario conoce, por ejemplo, una contraseña
- Algo que el usuario posee, por ejemplo, una tarjeta con banda magnética, en la que están grabados sus datos de identificación/autenticación.
- Alguna característica física, como la huella dactilar o la voz.

Autenticación fuerte: Proceso de autenticación que utiliza una combinación de dos de los mecanismos propios de la autenticación, como medio para reforzar la seguridad de dicho proceso.

Autenticidad: Característica por la que se garantiza la identidad del usuario que origina una información, es decir conocer con certeza quién envía o genera una información específica.

Autorización: Derecho o permiso que se otorga a una entidad del sistema para acceder a un recurso del sistema.

Brithish Standard 7799 (BS7799): Estándar británico sobre seguridad de la información dividido en dos partes. La primera parte es un código de mejores prácticas y provee directrices sobre cómo proteger los sistemas de información. La segunda parte establece las especificaciones de los sistemas de gestión de seguridad de la información.

Ciclo de vida informático: Ciclo que siguen los sistemas de información desde su creación hasta su eliminación. Dicho ciclo consta de las siguientes fases: fase de estudio de viabilidad, fase de análisis y definición de requisitos, fase de diseño y elaboración, fase de aceptación y pase a producción, fase de mantenimiento y fase de eliminación.

Cifrado: Proceso utilizado para transformar un texto a una forma ininteligible de manera que los datos originales no puedan ser recuperados (cifrado de una vía) o sólo puedan ser recuperados usando un proceso inverso de descifrado (cifrado de dos vías).

Código malicioso (malware): Cualquier software, macro, activex, javascript… cuyo objetivo sea causar daños a uno o varios de los siguientes elementos: equipos, sistemas informáticos, redes de comunicación y usuarios -sin el conocimiento de estos últimos- (ralentización del sistema, usos fraudulentos, robos de información…); como por ejemplo, virus, gusanos, troyanos, jokes (programas broma), hoaxes (bulos), bombas lógicas, spyware, adware, keyloggers, etc.

Confidencialidad: Característica que previene contra la puesta a disposición, comunicación y divulgación de información a individuos, entidades o procesos no autorizados.

Continuidad de negocio (actividad): Controles que aseguran que las operaciones informáticas y de actividad se mantienen sin interrupción, o reducen al mínimo el tiempo de ruptura de servicio, cuando ocurre un incidente o desastre.

Control de acceso: Proceso de limitación de los derechos o privilegios sobre los activos informáticos de un sistema o una red.

Control de seguridad: Mecanismo (técnico u organizativo) de salvaguarda que permite la reducción del riesgo de seguridad sobre un sistema, componente o proceso.

Copias de respaldo: Copia de información y software que permite la recuperación de los mismos en caso de pérdida.

Credencial: Datos transferidos o presentados para establecer tanto la identidad o la autorización de una entidad, ya sea una persona, un sistema de información o una aplicación concreta.

Criptografía: Ciencia matemática que estudia los algoritmos para asegurar la confidencialidad y autenticidad de datos mediante el proceso de reemplazarlos por una versión transformada. Esta puede ser reconvertida a la forma original sólo por alguien que posea el algoritmo criptográfico y las claves adecuadas.

También es el nombre que se le da a la disciplina que incluye los principios, medios y métodos para transformar los datos con intención de ocultar la información y prevenir la modificación y los usos no autorizados de la misma.

Cuerpo normativo de seguridad: Conjunto de documentación que establecen las prácticas y deberes de seguridad de una Organización. Está compuesto por la política de seguridad, normativa de seguridad, estándares de seguridad, procedimientos de seguridad y guías de seguridad.

Datos: Son una representación simbólica (numérica, alfabética, algorítmica, etc.), atributo o característica de una entidad. El dato no tiene valor semántico (sentido) en sí mismo, pero convenientemente tratado (procesado) se puede utilizar en la realización de cálculos o toma de decisiones. Dentro de la ITT, se utiliza el término dato para hacer referencia a la información de configuración de la ITT.

Descifrado: Operación que obtiene un texto original a partir de un texto cifrado.

Disociación (enmascaramiento) de datos: Proceso efectuado sobre los datos reales de personas para su tratamiento en entornos de prueba o elaboración y que consiste en la eliminación de las relaciones entre las personas y sus datos personales, creando otras ficticias, de tal modo que no se permita la identificación de estas.

Disponibilidad: Característica que asegura que los usuarios autorizados tienen acceso a la información y sus activos asociados cuando se requieran y previene contra intentos de denegar el uso autorizado a los mismos.

Dominio de seguridad: Un conjunto de elementos, una política de seguridad, una autoridad de seguridad y un conjunto de actividades pertinentes a la seguridad, donde el conjunto de elementos está sujeto a la política de seguridad, para las actividades especificadas y la política de seguridad es administrada por la autoridad de seguridad para el dominio de seguridad.

EDI (Electronic Data Interchange): Intercambio de datos de negocio entre sistemas de información de partners de negocio o instituciones gubernamentales en formatos estándares.

Estándar de seguridad: Contempla directrices específicas instauradas en la Organización relacionadas con aspectos concretos de seguridad tales como el uso de librerías criptográficas, la utilización de arquitecturas de seguridad ya implantadas, etc.

Externalización: Situación en la que un proceso de la Organización ha sido delegado en otra Organización, normalmente a través de un acuerdo de nivel de servicio.

Firma digital: Valor computado por un algoritmo criptográfico y añadido a un activo de información de forma que el recipiente de dicha información pueda comprobar la integridad y autenticidad de la misma.

Hardware: Componentes físicos de un sistema o equipo.

Identificación: Acto o proceso de presentar un identificador a un sistema para que el sistema pueda reconocer la entidad y distinguirla de otras entidades.

Impacto: Resultado, normalmente negativo, de la materialización de una amenaza de seguridad.

Imposibilidad de rechazo (no repudio): Característica de la información que participa en una transacción o envío que proporciona garantías para proteger al emisor contra la negación de recepción por parte del receptor y viceversa.

Información: Conjunto de datos que están organizados, que tienen un significado y que son tratados por la ITT. La información se considera un activo (ver definición de activo).

Integridad: Característica que asegura que la información no se ha transformado ni modificado de forma no autorizada durante su procesamiento, transporte o almacenamiento, detectando fácilmente posibles modificaciones que pudieran haberse producido.

ISO/IEC 27002:2005: Conjunto de controles que comprende las mejores prácticas en seguridad de la información. Es el resultado de la estandarización de la primera parte del BS7799.

Ley de Firma Electrónica: Ley que define el marco de validez de los mecanismos de firma digital para su uso en relaciones entre entidades.

Ley de los Servicios de la Sociedad de la Información (LSSI); Ley que tiene por objeto controlar la prestación de servicios a través de Internet, estableciendo medidas que aseguran la trazabilidad de las personas físicas responsables de los mismos.

Ley de Protección de Datos de Carácter Personal (LOPD): Ley que tiene por objeto garantizar y proteger el tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas.

Monitorización: Proceso de adquisición y análisis en tiempo real de las actividades de usuarios, sistemas o redes de la Organización, ya sea por personas o mediante herramientas automatizadas.

No repudio: ver imposibilidad de rechazo.

Normativa de seguridad: Compuesta por normas de carácter general derivadas de las directrices que forman la política de seguridad. Las normativas de seguridad atribuyen funciones y responsabilidades a figuras organizativas y establecen obligaciones y prohibiciones relativas a la seguridad de la información.

Plan de continuidad de actividad: Plan que define los procesos y responsabilidades de actuación en caso de incidente o desastre para recuperar el correcto funcionamiento de las operaciones informáticas y la actividad de la Organización.

Política de seguridad: Constituye las directrices básicas y duraderas de la seguridad de la información en una Organización. Estas directrices definen el marco de actuación de los siguientes niveles dentro del cuerpo normativo. Normalmente se trata de un documento breve y conciso que se toma como referencia para elaborar el resto del cuerpo normativo de seguridad.

Procedimiento de seguridad: Proporcionan las instrucciones detalladas para llevar a cabo las tareas relacionadas con la seguridad de la información. Los procedimientos tienen un ámbito reducido de actuación y tienen siempre carácter operativo. Los procedimientos complementan los estándares de seguridad aportando la operativa necesaria para cumplirlas.

Registro: Proceso de almacenamiento de la actividad de usuarios, sistemas o redes en un repositorio que permita su análisis posterior por personas o herramientas automatizadas.

Reglamento de Medidas de Seguridad: Conjunto de medidas organizativas y técnicas cuya implantación permite cumplir con la Ley Orgánica de Protección de Datos de Carácter Personal.

Respaldo de información: Proceso periódico de creación de copias de respaldo de la información y el software de los sistemas de información de la Organización.

Responsable de Seguridad: Figura organizativa encargada de la gestión y mantenimiento de la seguridad de la información en la Organización.

Restauración: Proceso de recuperación de información y software almacenados en las copias de respaldo en los sistemas de información originales debido a pérdida de dicha información o software ocurrida en los mismos.

Riesgo de seguridad: Situación en la que existe una vulnerabilidad de seguridad y un adversario potencial con la motivación y la capacidad para explotarla.

Segregación de tareas: Método consistente en la separación de la gestión o ejecución de ciertas tareas o áreas de responsabilidad para reducir las oportunidades de modificación no autorizada o de mal uso de la información o los servicios.

Seguimiento: Proceso que consiste en la comprobación periódica de la efectividad de los mecanismos de control implantados en la Organización.

Seguridad de los sistemas y tecnologías de la información: Conjunto de procesos y medidas cuya finalidad es prevenir de cualquier peligro, daño o riesgo la información para preservar su confidencialidad, integridad, disponibilidad, autenticidad y no repudio, así como los elementos (hardware, software, redes, datos y personal) que la transmiten, almacenan y procesan, impidiendo el funcionamiento indeseado de los mismos.

Service Level Agreement (SLA): Un SLA (Service Level Agreement) o ANS (Acuerdo de Nivel de Servicio) es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad del servicio. Básicamente define la relación entre ambas partes: proveedor y cliente. Un SLA identifica y define las necesidades del cliente a la vez que controla sus expectativas de servicio en relación a la capacidad del proveedor. El objetivo es proporcionar un marco de entendimiento, reducir las áreas de conflicto y favorecer el diálogo ante la disputa.

Software: Programas informáticos (almacenados y ejecutados por el hardware) y datos asociados (que son asimismo almacenados en hardware).

Tramitación telemática: La aplicación de las más modernas tecnologías a la tramitación de los procedimientos que permite la automatización de actuaciones que hasta ahora exigían la participación del personal funcionario o autoridad competente. La Administración facilitará a los ciudadanos el estado de tramitación de los procedimientos tramitados por medios telemáticos.

Teletrabajo: Trabajo realizado desde una situación remota (comúnmente desde casa) y conectando con la oficina a través de un ordenador personal equipado con un módem u otro mecanismo de conexión.

Vulnerabilidad de seguridad: Debilidad de un sistema de información, procedimientos de seguridad, controles internos, etc. que podría ser utilizada para producir un incidente de seguridad.