POLITICA SEGURIDAD DE LA UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA (ULPGC)

INDICE

0 Prólogo

En base a las exigencias legales vigentes en materia de Seguridad de la Información y a las necesidades y expectativas propias de la Universidad de Las Palmas de Gran Canaria en relación a la preservación de la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y conservación de la información manejada por la organización surge la presente Política de Seguridad. Este documento establece para los sistemas de información de la Universidad de Las Palmas de Gran Canaria las directrices mínimas en materia de seguridad, dotando 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 cuerpo de la Política de Seguridad queda estructurado en los siguientes apartados:

- Organización de la seguridad
- Planificación de la seguridad de la información
- Control de acceso a los sistemas de información
- Explotación segura de los sistemas de información
- Seguridad de los servicios externos
- Continuidad de los servicios prestados por los sistemas de información
- Monitorización de la seguridad
- Protección de instalaciones e infraestructuras
- Seguridad ligada al personal
- Seguridad del equipamiento y responsabilidades del usuario
- Protección de las comunicaciones
- Protección de los soportes de información
- Seguridad en las aplicaciones
- Protección de la información
- Protección de los servicios base

1 Introducción

Uno de los activos más valiosos de la Universidad de Las Palmas de Gran Canaria (en adelante ULPGC) es la información que trata en el ejercicio de su actividad. La presente Política de Seguridad está enfocada al mantenimiento de la seguridad de la información de la ULPGC durante su tratamiento por parte de los sistemas de información. 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 soporta estos sistemas de información.

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 diversas características relacionadas con la seguridad, que constituyen las garantías que se deben salvaguardar para cualquier información o documentación tratada por los sistemas de información:

- **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 y 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.
- **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 de la Política de Seguridad 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 ULPGC. Solo de esta manera se conseguirá preservar la información, salvaguardando las garantías descritas y cumpliendo las leyes que afectan a su tratamiento. Todo ello se desarrollará siguiendo un principio de proporcionalidad, en cuya virtud solo se exigirá la aplicación de las medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones.

2 Ámbito de aplicación

La ULPGC establece, dentro de su estrategia corporativa, la mejora en la calidad y eficiencia de su gestión como una de sus líneas estratégicas, para lo cual es imprescindible llevar a cabo un uso eficaz de los sistemas de información. Esta

utilización de los sistemas de información como base para el incremento en la eficiencia en la gestión supone un reto para la ULPGC, 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 ULPGC tiene la obligación de proteger la información de los ciudadanos, así como de cumplir con las leyes emergentes que condicionan el uso de las tecnologías de la información.

Para conseguir una mejora real en la calidad de la gestión va a ser imprescindible que la utilización de los sistemas de información ofrezca a todos los grupos de interés unas garantías mínimas de confianza en el uso de estos medios, constituyendo así mismo una de las piedras angulares para la mejora de la proyección social y reconocimiento de la ULPGC en materia de cercanía al ciudadano y de referencia en la prestación de servicios de e-Administración. Por este motivo se establece el cumplimiento de la presente Política de Seguridad como la base para la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos por parte de todos los grupos de interés.

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

- Los sistemas de información de la ULPGC, considerando todos los componentes necesarios para el correcto funcionamiento de los mismos, así como los propios componentes hardware y software que los componen.
- La información afectada que será la tratada por los sistemas de información, es decir, toda la información que utilizan, custodian o crean los empleados de la ULPGC, 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 estos o no en instalaciones propias.
- Los procesos organizativos referentes al uso e implantación de los sistemas de información que afectarán a empleados de la ULPGC.
- Las personas afectadas por la presente Política de Seguridad, serán:
    - Estudiantes de la ULPGC que hagan uso de los sistemas de información.
    - Personal de la ULPGC que hagan uso de los sistemas de información.
    - Desarrolladores e integradores de los sistemas de información de la ULPGC, entendiendo como tal cualquier persona participante en la creación o construcción de los sistemas de información, tanto propios como externos.
    - Administradores de recursos que dan soporte a los sistemas de información, entendidos como cualquier persona propia o externa que participa o tiene responsabilidades en el correcto funcionamiento de los sistemas de información de la ULPGC (administradores de sistemas, administradores de bases de datos, administradores de red, etc.).
    - Empleados: personal funcionario, laboral y eventual.
    - Externos: personal perteneciente a otras entidades del que, en virtud de relaciones especiales, como contratos de servicios, de asistencia técnica y de asesora, entre otras, hace uso la ULPGC.
    - Otros que puedan desarrollar alguna función que afecte a los sistemas de información, como las personas que se ocupan del mantenimiento de las áreas seguras.
    - En general, cualquier otra persona con algún tipo de vinculación con la ULPGC y que utilice o posea acceso a sus sistemas de información.

Por ello, la presente Política de Seguridad debe ser conocida y aplicada por todo el personal aquí reflejado, y su cumplimiento debe considerarse obligatorio para todo el personal implicado.

3 Política de Seguridad

Las directrices de la política de seguridad de la ULPGC han sido definidas de acuerdo con los estándares y reglamentaciones de seguridad aplicables, y en particular siguiendo las directrices del Real Decreto 3/2010, que establece un marco de referencia de seguridad respaldado legalmente y reconocido a nivel nacional. 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 ámbitos de seguridad que son cubiertos por la presente política de seguridad.

3.1 Organización

Dentro de este ámbito se recogen las directrices generales relacionadas con la organización de la seguridad dentro de la ULPGC, en concordancia con las exigencias regulatorias y normativas vigentes y con el compromiso de la ULPGC con la seguridad de sus sistemas de información. Así, la ULPGC entiende la seguridad como un proceso integral y continuo en el tiempo, excluyendo por tanto cualquier actuación puntual o tratamiento coyuntural en esta materia. Dicha seguridad está constituida por todos los elementos técnicos, humanos, materiales y organizativos necesarios para garantizar una adecuada gestión de la misma, articulándose medidas de seguridad que contemplan los aspectos de prevención, detección, reacción y recuperación, para conseguir reducir la posibilidad de materialización de las amenazas y que los incidentes de seguridad que se puedan producir se detecten y traten a tiempo y no afecten gravemente a la información que se maneja o los servicios que se prestan, permitiendo su restauración. Las medidas de seguridad dispuestas se reevalúan y actualizan periódicamente, con el fin de adecuar su eficacia a la constante evolución de los riesgos y los sistemas de protección existentes.

Con el fin de que la seguridad comprometa a todos los miembros de la organización, la ULPGC establece los siguientes roles y responsabilidades:

- **Responsables de la información y de los servicios**: Son los roles que deben establecer los requisitos de seguridad aplicables a la información y los servicios bajo su responsabilidad. Este rol estará ostentado por cada uno de los directores relacionados con los servicios electrónicos ofrecidos (Servicio de personal, Servicio de gestión académica, Servicio económico y financiero y Servicio de organización y régimen interno). Ostentarán las siguientes responsabilidades específicas:
    - Definir para la información y los servicios electrónicos bajo su responsabilidad las dimensiones de la seguridad relevantes (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) y su nivel correspondiente.

- Velar por la inclusión de cláusulas de seguridad en los contratos con terceras partes y por su cumplimiento.
- Colaborar en el análisis de impacto de los incidentes que se puedan producir y plantear las estrategias y salvaguardas ante los mismos.
- Cualquier otra función que pueda ser encomendada por los órganos correspondientes.

- **Responsable de la seguridad**: El responsable de la seguridad de la información tomará las decisiones necesarias para satisfacer los requisitos de seguridad establecidos por los responsables de la información y de los servicios. Este rol lo ostentará el Gerente, asumiendo las siguientes responsabilidades específicas:
  - Determinar las medidas de seguridad necesarias para la protección de la información manejada y los servicios prestados y verificar que las establecidas son adecuadas en todo momento.
  - Determinar la categoría del sistema y las medidas de seguridad que deben aplicarse.
  - Informar a los Responsables de la Información y de los Servicios de las incidencias de seguridad.
  - Reportar el estado de la seguridad al Comité de Seguridad de la Información.
  - Impulsar o instar la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
  - Llevar a cabo el seguimiento de la Política de Seguridad de la Información de manera operativa así como de la seguridad física y lógica de los recursos.
  - Cualquier otra función que pueda ser encomendada por los órganos correspondientes.

- **Responsable de los sistemas**: El responsable de los sistemas de información será el encargado de aplicar las medidas de seguridad de índole tecnológica determinadas por el Responsable de la seguridad. Este rol lo asumirá el Director del Servicio de Informática, asumiendo las siguientes responsabilidades específicas:
  - Garantizar que las tareas propias de la administración de la seguridad de los sistemas se llevan a cabo de manera correcta.
  - Garantizar que los sistemas de información permanecen bajo control.
  - Llevar a cabo los procesos de seguridad en el ámbito de su área.
  - Implementar la seguridad física y lógica dentro de su área.
  - Colaborar en las auditorias de seguridad y la gestión de riesgos.
  - Cualquier otra función que pueda ser encomendada por los órganos correspondientes.

- El **comité de seguridad** es el órgano colegiado que dirige, gestiona, coordina, establece y aprueba las actuaciones en materia de seguridad de la información. Este Comité estará compuesto por:
  - Los responsables de la información y de los servicios.
  - El responsable de la seguridad.
  - El responsable de los sistemas.
  - El Director del Servicio Jurídico (permanente o puntual).

- El vicegerente de RRHH (permanente o puntual).

Todas estas figuras se coordinarán entre sí, y será el órgano en el que se resolverán los conflictos que puedan surgir en la aplicación de esta Política de Seguridad o de las normativas y procedimientos que la desarrollen.

El Comité tiene las siguientes funciones y responsabilidades concretas:

- Divulgar la Política de Seguridad de la Información y las normativas e instrucciones de seguridad de la información aprobadas.
- Interpretar y resolver los conflictos surgidos en materia de seguridad de la información.
- Promover la mejora continua de la seguridad de la información.
- Proponer al Consejo de Gobierno la aprobación de las modificaciones de la Política de Seguridad.
- Elaborar e impulsar la estrategia y nuevas líneas de trabajo en lo que respecta a la seguridad de la información.
- Elaborar, revisar y hacer el seguimiento regularmente de la Política de Seguridad de la Información y demás normativas generales.
- Comunicar a los órganos competentes el incumplimiento de la Política de Seguridad de la Información y las normativas derivadas e instar, en su caso, la adopción de las medidas disciplinarias o de cualquier índole correspondiente.
- Supervisar y llevar a cabo el seguimiento del proceso de seguridad.
- Supervisar los incidentes de seguridad que se hayan podido producir y las medidas aplicadas en cada caso.

También se creará un **subcomité técnico de seguridad** como órgano de apoyo al Comité de Seguridad. Este órgano, presidido por el Responsable de los sistemas, y cuya composición vendrá determinada por él, será el órgano encargado de gestionar la seguridad de la información desde un punto de vista tecnológico y de reforzar la labor del comité de seguridad en este ámbito, desarrollando las siguientes funciones y responsabilidades concretas:

- Proponer las medidas técnicas de seguridad necesarias para la protección de la información manejada y los servicios prestados, verificando que las medidas establecidas son adecuadas en todo momento.
- Proponer la categoría del sistema y las medidas de seguridad técnica que deben aplicarse.
- Colaborar en la evaluación de las incidencias de seguridad.
- Reportar el estado de la seguridad técnica al Responsable de Seguridad.
- Colaborar en la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
- Colaborar en la divulgación de la Política de Seguridad de la Información y las normativas e instrucciones de seguridad de la información aprobadas.
- Colaborar en la resolución de conflictos surgidos en materia de seguridad de la información.
- Colaborar en la promoción de la mejora continua de la seguridad de la información.

- Proponer al Comité de Seguridad la aprobación de las modificaciones de las normativas y procedimientos de seguridad.
- Poner en práctica la estrategia y líneas de trabajo en lo que respecta a la seguridad de la información.
- Hacer el seguimiento regularmente de las normativas y procedimientos de seguridad.
- Colaborar en el seguimiento del proceso de seguridad.
- Colaborar en el seguimiento de los incidentes de seguridad que se hayan podido producir y las medidas aplicadas en cada caso.

El proceso de seguridad implantado por la ULPGC será actualizado y mejorado de forma continua, mediante la aplicación de una sistemática PDCA.

3.2 Planificación

En este ámbito se contemplan las directrices relacionadas con la planificación de la seguridad dentro de la ULPGC, tanto en lo referente al análisis y gestión de los riesgos de seguridad de la información como en lo relativo a la planificación general de la seguridad de los sistemas de información de la ULPGC.

La ULPGC entiende que la gestión de la seguridad está basada en la gestión de riesgos, cuyo objetivo debe ser mantener los niveles de riesgo dentro de unos niveles mínimos aceptables mediante el despliegue de las medidas de seguridad apropiadas. Por ello, el análisis y gestión de riesgos es una parte esencial del proceso de seguridad, y se mantiene permanentemente actualizado siguiendo lo dispuesto en la metodología de análisis y gestión de riesgos, Magerit.

La ULPGC establece su estrategia de protección de los sistemas de información en la constitución de múltiples capas de seguridad, compuestas por medidas de naturaleza organizativa, física y lógica, dispuestas de tal forma que si una de ellas falla la seguridad del sistema en su conjunto no sea comprometida. Además, los sistemas de información se diseñan de forma que garanticen la seguridad por defecto, considerando expresamente la seguridad en su arquitectura. Con este fin, la ULPGC tiene establecidas una serie de cláusulas contractuales que consideran expresamente la seguridad y valoran que los productos de seguridad informáticos y de comunicaciones sean acreedores de una certificación de seguridad “Common Criteria” para la funcionalidad para la que son utilizados.

3.3 Control de accesos

Este dominio cubre las directrices de la ULPGC relacionadas con el control de acceso a los sistemas de información, tanto en lo referente a la gestión de usuarios como en lo relativo a la gestión de permisos y mecanismos de autenticación. En términos generales, estas directrices establecen que el acceso a los sistemas de información debe estar controlado y limitado exclusivamente a los usuarios, procesos, dispositivos y sistemas de información que estén debidamente autorizados, de forma que se restrinja el acceso a las funciones permitidas.

Los identificadores de usuario utilizados en los sistemas de información se asignan de forma unívoca, de modo que cada identificador está asociado a un único usuario o proceso. Existe un procedimiento formal para gestionar las altas, bajas y modificaciones de usuario.

Los usuarios de la ULPGC cuentan con soluciones de control de acceso a los sistemas de información que permiten limitar el acceso a la información, siendo los responsables de los servicios los que determinan dicha autorización. Estas autorizaciones se otorgan de acuerdo a los principios generales de mínimo privilegio, necesidad de conocer y capacidad de autorizar.

Los mecanismos de autenticación utilizados se encuentran definidos en el procedimiento de gestión de usuarios.

3.4 Explotación

Dentro de este ámbito se recogen todas las directrices establecidas por la ULPGC en relación a las medidas de seguridad a considerar durante la explotación de los sistemas de información. Aquí se contempla tanto la configuración segura de los sistemas como su mantenimiento, de modo que se gestione la seguridad a lo largo de todo el ciclo de vida de los sistemas de información.

Todos los sistemas de información de la ULPGC son configurados inicialmente de forma segura, de modo que proporcionan exclusivamente las funcionalidades mínimas necesarias, se limita el acceso a ellas y se configuran de forma que su uso natural sea sencillo y seguro por defecto.

La instalación de cualquier componente físico o lógico de un sistema de información requiere una autorización formal previa. Se mantiene un inventario actualizado de todos los componentes de los sistemas de información instalados y sus responsables. Una vez puestos en producción existe una sistemática de mantenimiento de los sistemas de información que estipula las tareas de mantenimiento a llevar a cabo, de acuerdo a las directrices de los fabricantes, y que regula la gestión de las actualizaciones de seguridad en función de la vulnerabilidad y el riesgo asociados.

Los incidentes de seguridad que se producen, y en particular los asociados con malware, son registrados y tratados diligentemente, utilizándose dichos registros para la optimización de las medidas de seguridad implantadas.

3.5 Servicios externos

En este ámbito se contemplan las directrices definidas por la ULPGC en relación a la utilización de recursos externos a la organización, estableciendo como premisa general que la ULPGC sigue siendo en todo momento responsable de los riesgos en que se incurra por el uso de los servicios externos utilizados, de forma que la organización debe adoptar las medidas necesarias para poder ejercer dicha responsabilidad y mantener el control de las funciones delegadas.

La ULPGC exige, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados.

La ULPGC regula contractualmente la utilización de recursos externos a la organización, estableciendo en dichos contratos las características del servicio, las responsabilidades de cada parte, la calidad mínima exigible y las consecuencias del incumplimiento del contrato.

En relación al seguimiento y gestión diaria de los servicios externos utilizados, la ULPGC lleva a cabo un seguimiento periódico del cumplimiento de las obligaciones pactadas contractualmente, estableciendo con cada proveedor una sistemática específica para la coordinación del servicio, la monitorización de su calidad y la resolución de las desviaciones y conflictos que puedan surgir.

3.6 Continuidad

Dentro de este ámbito se recogen las directrices relacionadas con la continuidad de los servicios prestados por los sistemas de información de la ULPGC. Así, se establece como garantía básica que todos los sistemas de información disponen de copias de seguridad actualizadas periódicamente, y que la organización ha establecido los mecanismos necesarios para garantizar la continuidad de sus servicios informáticos y de comunicaciones en caso de pérdida de las infraestructuras originales. Estas copias de seguridad están en línea con el análisis de impacto de los servicios informáticos y de comunicaciones de la ULPGC, que identifica los requisitos de disponibilidad de cada servicio.

3.7 Monitorización

Este dominio cubre las directrices de la ULPGC relacionadas con la monitorización tanto de los propios sistemas de información como del uso que los usuarios hacen de ellos. En términos generales, estas directrices establecen la obligatoriedad de registrar la actividad de los usuarios durante su uso de los sistemas de información, con el nivel de detalle necesario para identificar actividades indebidas o no autorizadas salvaguardando al mismo tiempo los derechos de los usuarios.

La ULPGC tiene establecidas soluciones de monitorización de los sistemas que permiten supervisar su comportamiento y detectar/prevenir la intrusión en ellos. Así mismo, la organización cuenta con indicadores que permiten medir el grado de implantación, eficacia y eficiencia de las medidas de seguridad establecidas, tanto técnicas como organizativas y operativas.

3.8 Instalaciones e infraestructuras

En este ámbito se contemplan las directrices definidas por la ULPGC en relación a la protección de las instalaciones y las infraestructuras físicas, articuladas mediante el control de acceso físico y el acondicionamiento y protección frente a contingencias ambientales. En términos generales, estas directrices se resumen en que los sistemas de información se instalan en salas específicas y separadas, que deben permanecer

cerradas, dotadas de mecanismos de control de acceso, como llaves o claves, cuya distribución debe estar controlada.

Los servidores y el equipamiento de red principal están instalados en los CPDs de la ULPGC. El acceso a estas salas está controlado mediante tarjetas contactless, y todos los accesos a estas salas se registran. Al personal autorizado se le habilita su tarjeta contactless para que pueda realizar el acceso. Esta tarjeta es programada en la administración del edificio en que se ubica el CPD, mediante autorización por escrito del responsable técnico de seguridad. Todos los visitantes (personal no autorizado por defecto, tanto propio de la ULPGC como ajeno) son identificados previamente a dicho acceso.

Los CPDs de la ULPGC están equipados con sistemas de control y acondicionamiento que velan por el buen funcionamiento del equipamiento albergado en ellos, siguiendo lo dispuesto en las normativas y procedimientos de control de acceso físico y lógico.

3.9 Personal

Este ámbito contiene las directrices de la ULPGC en materia de gestión del personal, y contempla todos los aspectos relacionados con la formación y capacitación, la concienciación y difusión y la gestión de sus deberes y obligaciones. La ULPGC establece la obligación de que todo el personal afectado conozca sus deberes y obligaciones en materia de seguridad, y los respete en el ejercicio de sus funciones. Para ello, la ULPGC se compromete a regular formalmente estos deberes y obligaciones y a formar al personal sobre ellos, de modo que la seguridad de los sistemas de información sea respetada, aplicada y supervisada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida.

La ULPGC establece las funciones y obligaciones que en materia de seguridad son aplicables a cada puesto de trabajo, identificando las condiciones de confidencialidad a cumplir y las medidas disciplinarias asociadas en caso de incumplimiento.

La ULPGC también establece los requisitos que debe cumplir todo el personal que sin pertenecer a la organización está relacionado con ella y afectado por esta Política, como es el personal perteneciente a empresas subcontratadas u otro tipo de colaboradores o socios.

Así mismo, la ULPGC tiene un programa de formación y concienciación que garantiza que periódicamente todo el personal recibe la información necesaria para saber cómo realizar su trabajo de manera segura y cómo debe participar en la gestión de la seguridad de los sistemas de información y los incidentes que puedan producirse, con el fin de que ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas sean fuentes de riesgo para la seguridad.

3.10 Equipamiento y responsabilidades del usuario

Dentro de este ámbito se recogen las directrices relacionadas con la gestión segura del equipamiento y material puesto a disposición de los usuarios, en relación tanto a las obligaciones de la ULPGC al respecto como a las responsabilidades que los usuarios deben asumir durante su uso.

El personal debe velar porque el puesto de trabajo esté despejado, de modo que no haya más material sobre su mesa que el requerido para la actividad que se esté realizando en cada momento. Ese material se deberá guardar en un lugar cerrado, como armarios o cajones, cuando no se esté utilizando.

Los equipos portátiles, al tener la consideración de entornos inseguros, deberán contar con medidas de seguridad adicionales. Por una parte, estos equipos estarán equipados con un firewall personal, que limite su visibilidad y controle el acceso al equipo cuando se conecte a redes públicas. Por otra se habilitarán normativas para controlar los equipos portátiles que posee la organización, su responsable y su ubicación y para reportar incidentes relacionados con pérdidas o sustracciones de dichos equipos. Así mismo, sus usuarios también deberán limitar la información que contienen estos equipos, evitando, en la medida de lo posible, que contengan claves de acceso remoto a la red de la ULPGC.

3.11 Comunicaciones

Este dominio cubre las directrices de la ULPGC relacionadas con la gestión de las redes de comunicaciones, principalmente de cara a su interconexión con redes ajenas, que en general tendrán la consideración de entornos inseguros. En general, estas directrices se resumen en la obligatoriedad de proteger el perímetro de la red, en particular si se conectan a redes públicas, y de controlar los puntos de interconexión, aplicando medidas de seguridad en función de los riesgos derivados de dicha interconexión.

La ULPGC, según lo dispuesto en la arquitectura de seguridad, dispone de cortafuegos que separan las redes internas del exterior, de modo que cualquier tráfico entre redes internas y externas debe atravesarlos, estando configurados de forma que sólo se permiten los flujos de datos previamente autorizados.

3.12 Soportes de información

En este ámbito se contemplan las directrices definidas por la ULPGC en relación a la protección de los soportes de información, entendidos como todo el equipamiento móvil electrónico y no electrónico sobre el que se almacena información de forma estática (papel, pen-drives, CDs, DVDs, cintas, discos, etc.), que tendrán la consideración de entornos inseguros. Estas directrices se pueden resumir en tener la precaución de adoptar las medidas de seguridad pertinentes para proteger la información almacenada en estos dispositivos durante su uso y transporte, y garantizar su conservación y recuperabilidad a largo plazo.

Todo el personal de la ULPGC debe aplicar la debida diligencia y control a los soportes de información que permanezcan bajo su responsabilidad, garantizando que se cumplen las medidas de control de acceso físico y/o lógico aplicables y que se respetan unas exigencias ambientales mínimas apropiadas para su conservación.

Toda la información en soporte papel que haya sido causa o consecuencia de la información electrónica tratada por los sistemas de información deberá estar protegida con el mismo grado de seguridad que ésta, aplicando las medidas de seguridad apropiadas a la naturaleza del soporte en que se encuentren.

Los soportes de información electrónicos deberán estar etiquetados de forma que permitan identificar el nivel máximo de seguridad de la información contenida. Siempre que sea necesario su contenido deberá estar cifrado, y el responsable de sistemas deberá garantizar su control, registrando sus entradas y salidas y su eliminación segura.

3.13 Aplicaciones

Este ámbito contiene las directrices de la ULPGC en materia de desarrollo y puesta en producción de aplicaciones, que regulan los principales aspectos a considerar desde el punto de vista de la seguridad en torno a estas actividades.

En relación a la puesta en producción de aplicaciones, la ULPGC dispone de un entorno aislado en el que se llevan a cabo las pruebas, realizadas con datos previamente ofuscados. Estas pruebas contienen una parte funcional y otra parte de seguridad, en la que se verifica el cumplimiento de los criterios de aceptación en materia de seguridad y que su puesta en marcha no provoca deterioros en la seguridad de otros componentes del sistema de información afectado.

3.14 Información

Dentro de este ámbito se recogen las directrices de la ULPGC relacionadas con la protección de la información, relativas tanto a la protección específica de los datos de carácter personal de acuerdo a las exigencias del Reglamento de Desarrollo de la LOPD como a la protección general de toda la información electrónica gestionada por la ULPGC en el ejercicio de sus funciones.

La ULPGC cumple de forma escrupulosa las exigencias legales vigentes en materia de protección de datos de carácter personal, aplicando de manera global a esta información las medidas de protección preceptivas por dicha regulación, sin perjuicio de cumplir, además, otras medidas de seguridad adicionales en caso de que se considere necesario.

La ULPGC clasifica la información en virtud de su naturaleza, identificando responsables de la información de acuerdo a lo establecido en la presente Política. Los criterios de clasificación y designación de responsables están identificados en el procedimiento correspondiente, en base a los cuales estos responsables podrán modificar dicha clasificación.

Como norma general de protección de la información, la ULPGC establece la obligatoriedad de llevar a cabo copias de seguridad que permitan recuperar datos pasados. Así mismo, la organización establece la obligatoriedad de llevar a cabo procesos de limpieza de documentos, según los dispuesto en el procedimiento de borrado de metadatos.

La ULPGC ha desarrollado una Política de Firma Electrónica en la que establece las condiciones de uso de este mecanismo, así como las características generales que debe cumplir, según lo dispuesto en Ley de Firma Electrónica (LFE) 59/2003 del 19 de diciembre.

3.15 Servicios de base

En este ámbito se contemplan las directrices definidas por la ULPGC en relación a la protección de los servicios de base, teniendo esta consideración los servicios web y el servicio de correo electrónico prestados por la organización.

En general, la ULPGC tiene establecidas medidas preventivas y reactivas encaminadas a minimizar el impacto de los ataques informáticos para lo que ha desplegado granjas de servidores en lugares geográficamente distantes.

La ULPGC protege sus servicios de correo electrónico con sistemas anti-virus y anti-spam, y ha desarrollado una normativa de uso de correo electrónico que regula las normas de utilización de este servicio por parte de sus usuarios.

La organización también ha desplegado soluciones de protección de los servicios y aplicaciones web destinadas a la publicación de información, consistentes en el despliegue de arquitecturas y configuraciones seguras en estos servicios.

Todos los servicios web ofrecidos desde la ULPGC están albergados bajo los dominios controlados por la universidad. Los contenidos de las páginas web se ajustan en todo momento a los fines propios de la universidad, respetando en todo caso los principios contenidos en la Ley de Servicios de la Sociedad de la Información (LSSI). No deben publicarse en la página web contenidos cuyos derechos de difusión no correspondan al responsable de la página web, salvo que el autor y/o titular de los derechos de difusión haya consentido expresamente en su publicación.

4 Desarrollo y despliegue de la Política de Seguridad

La presente Política de Seguridad se desarrollará en una serie de documentos normativos en los que se recogerán políticas de seguridad específicas para los distintos ámbitos contemplados.

Se desarrollan y aprueban diferentes políticas, normativas y regulaciones específicas. En caso de que la normativa desarrollada afecte de manera general a los usuarios de los sistemas de información de la ULPGC, dicha afección deberá ser previamente aprobada por el Comité de Seguridad.

Las políticas, normativas y regulaciones específicas que se aprueban se notifican y difunden apropiadamente a todos los afectados.

Al menos es necesario desarrollar las siguientes normativas y procedimientos:

- Normativa general utilización recursos y sistemas de información.
- Normativa de uso de correo electrónico.
- Normativa de acceso a internet.
- Normativa de creación y uso de contraseñas.
- Normativa para trabajar fuera de las instalaciones.
- Normativa de gestión de usuarios.
- Normativa de control de acceso lógico.
- Procedimiento de control de acceso físico.
- Procedimiento de clasificación y tratamiento de la información.

- Procedimiento de autorizaciones.
- Procedimiento de gestión de usuarios.
- Procedimiento de gestión de incidentes de seguridad.

Anexo I: Glosario de términos

A continuación se describe el significado de los diferentes términos más usuales pertenecientes al vocabulario de la seguridad de la información que aparecen en el presente documento.

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

Sistema de información: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Categoría de un sistema: es un nivel dentro de la escala básica-media-alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

Medidas de seguridad: conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Análisis de riesgos: utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Gestión de riesgos: actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente se seguridad: suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Proceso: conjunto organizado de actividades que se llevan a cabo para producir a un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

LFE (Ley de Firma Electrónica): LEY 59/2003, del 19 de diciembre, que otorga a la firma electrónica el mismo valor a efectos legales que la firma manuscrita. La Firma Electrónica, puede vincularse a un documento para identificar al autor, para señalar conformidad (o disconformidad) con el contenido, para indicar que se ha leído o, según el tipo de firma, garantizar que no se pueda modificar su contenido.

LSSI (Ley de Servicios de la Sociedad de la Información) o LSSICE (Ley de Servicios de la Sociedad de Información y Comercio Electrónico): Ley que establece las obligaciones, responsabilidades, infracciones y sanciones de aquellas empresas y

particulares en general que tienen una página Web o que operan por Internet. También regula expresamente el envío de correos electrónicos con fines comerciales.

Sistemática PDCA: La sistemática PDCA es un proceso de mejora continua basado en un ciclo de planificación, realización, revisión y actuación, que se puede usar para mejoras "incrementales" y "radicales". La sistemática PDCA es un instrumento clásico para el incremento de la eficiencia en la empresa y la optimización de todos los procedimientos y procesos.

Áreas seguras: Son sectores concretos de las instalaciones, que exigen medidas específicas de seguridad. Espacio delimitado por barreras físicas y de acceso controlado, en el que se ejerce un cierto control sobre movimientos y permanencia de los activos.

Common criteria (CC): La norma Common Criteria (ISO/IEC 15408) proporciona un marco estandarizado (metodología, notación y sintaxis) para especificar y verificar los requisitos funcionales de seguridad que debe cumplir un producto o sistema TI y las medidas de garantía aplicadas sobre los mismos, en sus diferentes fases del ciclo de vida.