POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Universidad de Jaén

Revisado:	Servicio de Información y Asuntos Generales	
	Servicio de Informática	
Versión: 1.0	**Fecha Versión:**26/03/2015	**Nº Total Páginas:** 18
Aprobado por: Consejo de Gobierno	**Fecha Aprobación:** 26/03/2015	

Contenido

1. Aprobación y entrada en vigor

Texto aprobado el día 26/03/2015 por el Consejo de Gobierno.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva versión de la misma.

2. Introducción

La Universidad de Jaén depende de los sistemas de Información (SI) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los Sistemas de Información deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

La Universidad de Jaén debe cerciorarse de que la seguridad es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para todos los proyectos que se relacionen con los Sistemas de Información.

La Universidad de Jaén debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

2.1. Prevención

La Universidad de Jaén debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, se debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. Respuesta

La Universidad de Jaén:

- Establecerá mecanismos para responder eficazmente a los incidentes de seguridad.
- Designará un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecerá protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, la Universidad de Jaén dispondrá de planes de continuidad de los sistemas de Información como parte de su plan general de continuidad del servicio y actividades de recuperación.

3. Alcance

Esta política se aplica a los sistemas de Información de la Universidad de Jaén y a todos los miembros de la organización, que tengan relación con los servicios de administración electrónica:

- Web Institucional (CRUE_05_01)
- Tablón de Anuncios (SR02)
- Gestión Económica. Perfil del contratante (SR03)
- Secretaria General. Firma electrónica (SR_FirmaElec)
- Verifirma (SR05)
- Secretaria General. Registro (CRUE_03_43)
- Gestión Académica. Becas (CRUE_03_06)
- Gestión Académica. Automatrícula (CRUE_03_05)
- Autenticacion centralizada (SIDUJA) (CRUE_08_04)
- Secretaria General. Convenios (CRUE_03_45)
- Extensión Universitaria. Actividades Deportivas (CRUE_03_36)
- Investigación y transferencia: Portal del investigador (SR12)

4. Declaración de la política de seguridad de la información

El propósito de esta Política de la Seguridad de la Información es proteger la información y los servicios de administración electrónica de la Universidad de Jaén.

Es la política de esta entidad asegurar que:

- La información y los servicios están protegidos contra pérdidas de disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad.
- La información está protegida contra accesos no autorizados.
- Se cumplen los requisitos legales aplicables.
- Se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Las incidencias de seguridad son comunicadas y tratadas apropiadamente.
- Se establecen procedimientos para cumplir con esta Política.
- El Responsable de Seguridad de la Información será el encargado de mantener esta política, los procedimientos y de proporcionar apoyo en su implementación.
- El Responsable de Servicio será el encargado de implementar esta Política y sus correspondientes procedimientos.
- Cada empleado es responsable de cumplir esta Política y sus procedimientos según aplique a su puesto.
- La Universidad de Jaén implementa, mantiene y realiza un seguimiento del Esquema Nacional de Seguridad.

5. Misión de la Universidad de Jaén

La misión de la Universidad de Jaén se encuentra detallada en http://www10.ujaen.es/conocenos/organos-gobierno/ptransparencia/informacion-institucional/mision-vision-y-valores

6. Marco Normativo

La legislación aplicable a la Universidad se encuentra detallada en el siguiente enlace: http://www10.ujaen.es/conocenos/servicios-unidades/sinformatica/calidad/legislacion

7. Organización de la seguridad

7.1. Comité: Funciones y Responsabilidades

El Comité de Seguridad de la Información estará formado por:

Presidente: La persona designada como Responsable de la Información.

Secretario: La persona designada como Responsable de Seguridad, quién se encargará de convocar, preparar, redactar las actas de reunión del Comité y realizar el seguimiento de las decisiones adoptadas.

Vocales:

La persona designada como Responsable del Fichero

La persona designada como Responsable de Servicios

La persona designada como Responsable del Sistema

Dos personas designadas como Responsables de Seguridad delegados

Vicerrector TIC o quien tenga atribuidas las funciones.

Se han definido las siguientes responsabilidades:

- Responsable de la Información (ENS) - Rector
- Responsable de Seguridad (ENS y LOPD) - Secretario General delegado en jefe del Servicio de Información y Asuntos Generales
- Responsable del Fichero (LOPD) - Secretario General
- Responsable de los Servicios (ENS) - Gerente
- Responsable del Sistema (ENS) - Jefa del servicio de informática
- Responsable de Seguridad delegados - Jefes de cada Servicio

El Comité de Seguridad de la Información coordina la seguridad de la información en la Universidad de Jaén.

El Comité de Seguridad reportará al Consejo de Dirección de la Universidad de Jaén y tendrá las siguientes funciones:

- Informar regularmente del estado de la seguridad de la información al Consejo de Dirección.

- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Universidad de Jaén en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por el Consejo de Dirección.
- Proponer la normativa de seguridad de la información al Equipo de Gobierno para su aprobación.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Elaborar Planes de concienciación y formación.
- Analizar los principales riesgos residuales asumidos por la Universidad de Jaén y recomendar posibles actuaciones respecto de ellos.
- Analizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la Universidad de Jaén. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos de implantación de sistemas de información desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas de información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Coordinar y aprobar Planes de continuidad.

7.2. Roles: Funciones y Responsabilidades

Las funciones y responsabilidades se detallan en el **Anexo I**

7.3. Procedimientos de designación

El Consejo de Dirección designará las personas que ocuparán los roles definidos en esta Política así como la composición del Comité de Seguridad de la Información.

Los nombramientos se revisarán o renovarán con la revisión de la Política de Seguridad.

7.4. Revisión de la Política de Seguridad de la Información

Será misión del Comité de Seguridad de la información la revisión bienal de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el Consejo de Gobierno y difundida para que la conozcan todas las partes afectadas.

8. Datos de carácter personal

Todos los sistemas de información de la Universidad de Jaén que contienen datos de carácter personal han adoptado las medidas de seguridad exigidas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD.

Los ficheros afectados y los responsables correspondientes se encuentran recogidos en el Documento de Seguridad que se puede consultar en Universidad Virtual (https://uvirtual.ujaen.es)

Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la Universidad de Jaén.

9. Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

10. Desarrollo de la Política de Seguridad de la Información

Esta Política de Seguridad complementa las políticas de seguridad en diferentes materias. Se desarrollará en la normativa descrita en el **Anexo II** y por medio de procedimientos de seguridad que afrontan aspectos específicos. Los procedimientos de seguridad deben ser conocidos por aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Los procedimientos de seguridad estarán disponibles en Universidad Virtual (https://uvirtual.ujaen.es)

11. Obligaciones del personal

Todos los miembros de la Universidad de Jaén tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Se realizarán periódicamente acciones de concienciación y sensibilización en materia de seguridad de la información que afecte a todos los miembros de la Universidad de Jaén. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

12. Terceras partes

Cuando la Universidad de Jaén preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Universidad de Jaén utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Anexo I: Funciones y responsabilidades

Función	Responsabilidades
Responsable del Fichero	• Notificar los ficheros ante el Registro General de Protección de Datos para que se proceda a su inscripción. • Asegurarse de que los datos sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados. • Garantizar el cumplimiento de los deberes de secreto y seguridad. • Informar a los titulares de los datos personales en la recogida de éstos. • Obtener el consentimiento para el tratamiento de los datos personales. • Facilitar y garantizar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. • Asegurar que en sus relaciones con terceros que le presten servicios, que comporten el acceso a datos personales, se cumpla lo dispuesto en la LOPD. • Cumplir, cuando proceda, con lo dispuesto en la legislación sectorial que le sea de aplicación. • Garantizar el cumplimiento de los deberes de secreto y seguridad.
Responsable de la Información	• Velar por el buen uso de la información y, por tanto, de su protección, incluidos los ficheros de datos de carácter personal. • Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad. • Establecer los requisitos de la información en materia de seguridad. • Determinar los niveles de seguridad de la información. • Determinación de los niveles de seguridad requeridos en cada dimensión junto con el responsable del servicio. • Aceptación del riesgo residual junto con el responsable del servicio.
Responsable del Servicio	• Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad. • Determinar los niveles de seguridad de los servicios.
Responsable de Seguridad	• Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.

	• Promover la formación y concienciación en materia de seguridad de la información y protección de datos de carácter personal. • Determinación de la categoría del sistema. • Análisis de riesgos. • Declaración de aplicabilidad. • Medidas de seguridad adicionales. • Elaborar configuración de seguridad. • Documentación de seguridad del sistema. • Elaborar y aprobar procedimientos operativos de seguridad. • Elaborar planes de mejora de la seguridad junto con el responsable del sistema. • Elaborar planes de concienciación y formación. • Validar planes de continuidad. • Aprobar ciclo de vida de los sistemas de información: especificación, arquitectura, desarrollo, operación, cambios.
Responsable del Sistema	• Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento. • Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo. • Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad. • La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información. • La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información. • La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado. • La aplicación de los Procedimientos Operativos de Seguridad. • Aprobar los cambios en la configuración vigente del Sistema de Información. • Velar para que los controles de seguridad establecidos sean cumplidos estrictamente. • Velar para que son aplicados los procedimientos aprobados para manejar el sistema de información. • Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes. • Monitorizar el estado de seguridad del sistema proporcionado por las

	herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema y reportarlos el responsable de seguridad. ● Informar a los Responsables de la Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad. ● Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución. ● Aplicar configuración de seguridad. ● Implantación de las medidas de seguridad. ● Aplicar procedimientos operativos de seguridad. ● Monitorizar el estado de la seguridad del sistema y los reporta al responsable de seguridad. ● Elaborar y realizar ejercicios periódicos de los planes de continuidad. ● Elaborar Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios.

Anexo II: Normativa de Seguridad de los Sistemas de Información

II.1. Política de uso aceptable

Los sistemas de información y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de los usuarios. No se considera aceptable:

- La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Instalar, modificar o cambiar la configuración de los sistemas de software que no sea el permitido y necesario para el desarrollo del trabajo por parte del personal de la Universidad de Jaén (sólo los administradores de sistemas están autorizados a ello).
- No cumplir las condiciones de las licencias de todo software utilizado en el desarrollo de su trabajo.
- Queda prohibido el uso de equipos, redes y servicios para fines personales. En tal caso, será bajo la responsabilidad del usuario.
- Facilitar el acceso a las instalaciones o los servicios restringidos a personas no autorizadas.
- Malgastar los recursos de la red de manera premeditada.
- Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
- Introducir virus u otras formas de software malicioso adrede. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda causar molestar u ofender.
- Enviar mensajes de correo muy grandes o a un grupo muy numeroso de personas (que pueda llegar a saturar las comunicaciones).
- No verificar que los correos están libres de virus

II.2. Seguridad de la gestión de recursos Humanos

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

Se requerirá la firma de un acuerdo de confidencialidad para todos los empleados para evitar la divulgación de información secreta.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios terceros si procede.

Cuando se termine la relación laboral o contractual con empleados o personal externo (exceptuando los casos autorizados por el Responsable de Seguridad), se les retirarán los permisos de acceso a las instalaciones y la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

II.3. Seguridad física y del entorno

Para que una seguridad lógica sea efectiva es primordial que las instalaciones mantengan una correcta seguridad física para evitar los accesos no autorizados así como cualquier otro tipo de daño o interferencia externa.

II.3.1. Áreas restringidas

La Universidad de Jaén tomará las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones restringidas.

La totalidad de las instalaciones de la Universidad de Jaén cuentan con las barreras físicas necesarias para asegurar los recursos que éstas alberguen.

Los lugares donde se ubican los servidores y el cableado se considerarán áreas restringidas.

Las ventanas y puertas deberán permanecer cerradas cuando las instalaciones estén vacías.

Para la prevención de fugas de agua e inundaciones será necesaria la revisión periódica de la grifería, sanitarios y demás instalaciones que puedan causar daños de este tipo.

II.3.2. Seguridad de los equipos

Los equipos informáticos son un activo importante del que depende la continuidad de las actividades, por lo que serán protegidos de manera adecuada y eficaz.

Los equipos informáticos críticos de la Universidad de Jaén estarán protegidos contra posibles fallos de energía u otras anomalías eléctricas, para ello se habilitarán sistemas de alimentación ininterrumpida.

Los equipos deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento y su perfecto estado de forma para que mantengan la confidencialidad, integridad y sobre todo la disponibilidad de la información. Para ello deben someterse a las revisiones recomendadas por el suministrador.

Sólo el personal debidamente autorizado podrá acceder al equipo para proceder a su reparación.

También será necesario adoptar las medidas de precaución necesarias en caso de que los equipos deban abandonar las instalaciones para su mantenimiento.

II.4. Gestión de comunicaciones y operaciones

II.4.1. Procedimientos operativos y responsabilidades

La Universidad de Jaén controlará el acceso a los servicios en redes internas y externas y se asegurará de que los usuarios no ponen en riesgo dichos servicios. Para ello deberá establecer las interfaces adecuadas entre la red de la Universidad de Jaén y otras redes, los mecanismos adecuados de autenticación para usuarios y equipos, y los accesos para cada usuario del sistema de información.

Para evitar un uso malicioso de la red de la Universidad de Jaén existirán mecanismos para cubrir los servicios en red a los que se puede acceder, los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

Todos los empleados autorizados para el manejo de información automatizada deberán estar registrados como usuarios del sistema. Cada vez que accedan al sistema de información deberán validarse con su nombre de usuario, que será único e intransferible, y su contraseña personal. Esta contraseña caducará periódicamente.

Para asegurar la operación correcta y segura de los sistemas de información, los procedimientos de operación estarán debidamente documentados y se implementarán de acuerdo a estos procedimientos. Estos procedimientos serán revisados y convenientemente modificados cuando haya cambios significativos en los equipos o el software que así lo requieran.

II.4.2. Protección frente a código malicioso y código móvil

El Administrador del Sistema instalará las herramientas informáticas adecuadas para la protección de los sistemas contra virus, gusanos, troyanos, etc. y los usuarios deberán seguir las directrices que se les indiquen para proteger los equipos, aplicaciones e información con los que trabajan.

II.4.3. Copias de seguridad

La salvaguarda de la información almacenada en los PC será responsabilidad del usuario del mismo.

Para la salvaguarda de la información almacenada en servidores, se definirán procedimientos de copias de datos. Estas copias estarán claramente identificadas y depositadas en sitio seguro. También se desarrollarán procedimientos para recuperar los datos a partir de las copias de seguridad. Hay que asegurarse periódicamente de que la información se guarda correctamente y permite recuperar un nivel mínimo de servicio en caso necesario.

II.4.4. Gestión de la seguridad de la red

Los elementos de red (switch, router...) permanecerán fuera del acceso del personal no autorizado para evitar usos malintencionados que puedan poner en peligro la seguridad del sistema.

II.4.5. Gestión de soportes

Los usuarios aplicarán las mismas medidas de seguridad a los soportes (tanto papel como digitales) que contengan información sensible que a los ficheros de donde han sido extraídos.

Los soportes que contengan información sensible deben permanecer en cajones o armarios cerrados bajo llave. Cuando alguna persona autorizada deba utilizarla para realizar alguna gestión relacionada con las labores propias de la Universidad de Jaén, ésta se hará responsable del buen cuidado de los soportes. No los dejará encima de su mesa cuando abandone su puesto de trabajo ni los colocará en cualquier otro lugar donde una persona sin autorización pueda verlos o apropiarse de ellos.

Los soportes reutilizables cuya información ya no se necesite deberá borrarse, siempre que se cuente con la autorización precisa. Esta eliminación debe hacerse de forma segura para que los datos que contiene no se filtren a otras personas.

Siempre será necesario registrar la eliminación de soportes que contengan información sensible para mantener una pista de auditoría.

II.4.6. Intercambio de información

Se establecerán procedimientos para proteger la información que se intercambie a través de cualquier medio de comunicación (electrónico, verbal, fax, etc.).

II.4.7. Seguimiento

Según se considere necesario, se establecerán los mecanismos que permitan detectar actividades de proceso de información no autorizadas. Esto implicará realizar tareas para llevar a cabo controles e inspecciones de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y los procedimientos operativos así como para recomendar cualquier cambio que se estime necesario.

II.5. Control de accesos

II.5.1. Requisitos del servicio para el control de accesos

La información debe estar protegida contra accesos no autorizados. El Responsable del Servicio definirá las necesidades de acceso a la información a dos niveles, para el conjunto del área y las de cada usuario dentro del conjunto. Sólo se facilitará el acceso a la información necesaria para el trabajo a desarrollar.

También deben protegerse los puntos de entrada y salida de correo postal.

En el caso de que visitantes o personal no autorizado acceda a las instalaciones restringidas o a la información de la Universidad de Jaén deberá ir siempre acompañado por un miembro responsable de la Organización que controlará en todo momento que la seguridad de los recursos está garantizada.

II.5.2. Gestión de accesos a los sistemas de información

El administrador del sistema es responsable de proporcionar a los usuarios el acceso a los recursos informáticos, así como el acceso lógico especializado de los recursos (servidores, enrutadores, bases de datos, etc.) conectados a la red.

Los autenticadores se cambiarán con una periodicidad.

Cada usuario deberá estar asociado a un perfil, de acuerdo a las tareas que desempeña en la organización, definido por su responsable directo. Cada uno de estos perfiles dispondrá de unos determinados permisos y verá restringido su acceso a Información y sistemas que no le son necesarios para las competencias de su trabajo.

II.5.3. Control de acceso a los equipos

Los puestos de trabajo del personal deben estar despejados de papeles y otros medios de almacenamiento de la información para reducir los riesgos de acceso no autorizado así como otros posibles daños. Éstos deberían guardarse en espacios cerrados adecuados, especialmente fuera del horario laboral.

Los usuarios velarán por la seguridad en el acceso a su equipo informático y habilitarán contraseñas a tal efecto. De igual forma, es necesario configurar los equipos informáticos para que éstos queden bloqueados cuando el usuario no se encuentra en su puesto de trabajo de forma que sea necesario introducir una contraseña para acceder a los datos que se almacenan en el terminal.

También deben protegerse las máquinas de fax y las impresoras que no se encuentren atendidas por alguna persona de la Universidad de Jaén.

II.5.4. Control de acceso a la red

No se permitirá el acceso a la red oficial, a los sistemas, aplicaciones o información a ningún usuario que no esté formalmente autorizado para ello.

En el caso de proveedores de servicios o entidades externas, que necesiten acceder a ellos por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con la Universidad de Jaén para mantener el nivel de seguridad que se determine.

II.6. Uso de la información fuera de la Universidad

En caso de necesitar trabajar fuera de la Universidad con información en soporte electrónico o papel, se transportará con el debido cuidado.

Debido a los riesgos de seguridad en Internet, la transmisión de información de la organización al exterior, se realizará mediante una conexión segura (VPN). Antes de usar cualquier información hay que asegurarse de que el equipo en el que va a ser tratada está libre de virus o código malicioso.

Cuando los equipos o la información propiedad de la Universidad de Jaén están fuera de las instalaciones, el responsable de su seguridad es el empleado que los está utilizando y debe tomar las medidas pertinentes para evitar robos o daños durante su manipulación, transporte y almacenamiento.

II.7. Gestión de incidencias

Se habilitará un sistema de gestión de incidencias de seguridad que facilitará que cualquier empleado comunique las incidencias que sospeche u observe, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.).

Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.

El registro de incidencias servirá de base para identificar riesgos nuevos y para comprobar la eficacia de los controles implantados.

II.8. Continuidad del servicio

Es imprescindible para la Universidad de Jaén establecer las pautas de actuación a seguir en caso de que se produzca una interrupción de las actividades por fallos graves en la seguridad o desastres de cualquier tipo.

Para garantizar la continuidad de la actividad en estos casos, la Universidad de Jaén dispondrá de planes de contingencia que permitan la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo. La gestión de la continuidad del servicio incluirá, por tanto, diversos controles para la identificación y reducción de riesgos y un procedimiento que limite las consecuencias dañinas de los mismos y asegure la reanudación de las actividades esenciales en el menor tiempo posible.

La estrategia de continuidad del servicio se documentará, partiendo de los riesgos detectados y de los controles definidos en consecuencia que deberán probarse y actualizarse regularmente para comprobar su idoneidad.

La gestión de la continuidad del servicio se incorporará a los procesos de la Universidad de Jaén y será responsabilidad de una o varias personas dentro de la entidad.