SEGURIDAD DE LA INFORMACIÓN

APROBADO POR:	Nº DE REVISIÓN	FECHA	RESUMEN DE CAMBIOS/COMENTARIOS
Responsable de Seguridad	1	13/12/2013	Implantación Inicial
	1.1	10/05/2016	Actualizado el procedimiento para adecuarse a las modificaciones del ENS
Aprobado por el Comité de Seguridad	1.2	26/09/2017	Revisado por el Comité de Seguridad

Índice

1 OBJETO

Este procedimiento tiene por objeto describir el sistema establecido por la UGR para definir y regular las actividades, criterios y responsabilidades necesarias para gestionar la seguridad de la información.

2 ALCANCE.

Este procedimiento es de aplicación a todos los activos (y personal) que intervienen en la prestación de servicios incluidos en el Inventario de Activos.

3 DOCUMENTACIÓN DE REFERENCIA.

-Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

-Real Decreto 3/2010, de 8 de enero (BOE de 29 de enero), por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

-Real Decreto 1720/2007 de 21 de diciembre por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

-Política de Seguridad

-CCN-CERT Guía 802 - Auditoría del Esquema Nacional de Seguridad

4 RESPONSABILIDADES.

4.1 Responsable del Sistema.

-Aportar los recursos necesarios para el cumplimiento del Procedimiento

-Definir objetivos de cumplimiento

-Coordinar y supervisar la correcta ejecución del procedimiento

-Controlar que las incidencias se solucionan correctamente.

4.2 Responsable de Seguridad, Responsable de la Información, Administrador de la Seguridad del Sistema.

-Planificará las tareas necesarias para la seguridad de la información

-Asignará tareas al personal correspondiente

-Supervisará la realización del plan y tomará la medidas oportunas para corregir las desviaciones

4.3 Resto de Personal

-Ejecutar las tareas que les sean encomendadas y reportar las incidencias al Responsable de Seguridad.

5 DEFINICIONES.

Firma electrónica. Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Gestión de incidentes. Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

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

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

Política de firma electrónica. Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

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

Seguridad de las redes y de la información, es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

6 DESARROLLO.

6.1 Arquitectura de seguridad

Siempre en base a la información del Inventario de Activos

Planificación de la seguridad

La herramienta fundamental para la planificación de las acciones necesarias para mantener el nivel de seguridad requerido por la UGR es el **Análisis de Riesgos**, que se realiza según lo descrito en el ***<PSI02: Procedimiento de Análisis y Gestión de Riesgos>***.

6.1.1 Gestión de la capacidad

Para asegurar que se cuenta siempre con la capacidad necesaria para responder a las necesidades de los usuarios de nuestros servicios, para cada proyecto de implantación de nuevos sistemas se analizan las capacidades necesarias junto con los datos de la capacidad existente. Asimismo se analizan cuáles son los requisitos que se deben cumplir para poder suministrar los servicios ofertados con el nivel requerido, incluyendo estos requisitos en los pliegos de contratación cuando proceda.

En particular, se deberán identificar los siguientes requisitos:

•Si la capacidad de almacenaje es suficiente para los datos y las aplicaciones utilizadas

•Si la capacidad de procesamiento es suficiente para las transacciones a realizar

•Si existe una correcta distribución de la carga de trabajo entre los recursos disponibles

•Si hay soporte para atender de manera correcta las incidencias

•Si se han producido variaciones imprevistas en cualquiera de los parámetros anteriormente descritos

En los sistemas en explotación se controlará anualmente la capacidad utilizada y la prevista.

Se describirá más detalladamente en el ***<RG-06-CAPA: Plan de capacidad>***.

6.1.2 Gestión de compras

Tanto las compras como las subcontrataciones siguen un proceso regulado documentado formalmente, el ***<PE02-26-COMP: Procedimiento de compras y homologación de proveedores>*** de la ISO 9001 del CSIRC**.** Cuando los contratos incluyen acuerdos de nivel de servicio (ANSs o SLAs), se estipula asimismo el control del cumplimiento del mismo y las sanciones por incumplimiento, según lo descrito en ese procedimiento de Compras y Homologación de Proveedores.

6.2 CONTROL DE ACCESOS

Se clasifican los mecanismos de autenticación en tres tipos:

- "algo que se sabe": contraseñas o claves concertadas.
- "algo que se tiene": componentes lógicos (como certificados software) o dispositivos físicos (tokens).
- "algo que se es": elementos biométricos (huella digital).

Los mecanismos de autenticación se adecuarán al nivel del sistema atendiendo a las siguientes consideraciones:

- Para los sistemas de nivel bajo, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor. Por ejemplo usuario y contraseña.
- Para los sistemas de nivel medio se exigirá el uso de al menos dos factores de autenticación.
    - Presencial, verificando la identidad del usuario.
    - Telemático, usando certificado electrónico cualificado, mediante autenticación con una credencial electrónica obtenida tras un registro previo presencial (como el DNI electrónico o el certificado digital de Persona Física de la FNMT).

El control de los accesos queda descrito en los siguientes procedimientos de la ISO 9001 del CSIRC.

Los accesos locales se rigen por lo descrito en los siguientes procedimientos:

- ***<PE02-17-PSRC: Gestión de los servicios de redes de comunicaciones de UGR>***
- ***<PE02-21-GASR: Gestión, administración y soporte de la red UGR>***
- ***<PE02-24-BBDD: Administración y gestión de sistemas de bases de datos corporativos>***
- ***<PE02-22-GSRA: Gestión y administración de sistemas y redes de almacenamiento y despliegue de servicios TIC >***

Los accesos remotos se realizan mediante VPNs tal y como se detalla en los procedimientos de:

- ***<PE02-21-GASR: Gestión, administración y soporte de la red UGR>***
- ***<PE02-17-PSRC: Gestión de los servicios de redes de comunicaciones de UGR>***

6.2.1 Política de contraseñas

Las contraseñas de usuario se recomiendan ser cambiadas tras el primer acceso.

Las contraseñas de administración de los sistemas definidas por defecto, se cambiarán en el primer acceso para evitar la posibilidad de accesos no autorizados a través de su utilización, incluyendo, al menos:

oCuentas de los sistemas operativos.

oCuentas de acceso a la gestión de routers y firewalls.

oCommunity por defecto de los dispositivos SNMP ("public").

oCuentas por defecto de usuarios creados por aplicaciones y/o servicios.

Las contraseñas deben cumplir los siguientes requisitos:

oLongitud mínima de la contraseña: 6 caracteres y 8 para las cuentas con permisos de administración

oIncluir caracteres de tres de las siguientes categorías:

▪Mayúsculas (de la A a la Z)

▪Minúsculas (de la a a la z)

▪Dígitos de base 10 (del 0 al 9)

▪Caracteres no alfanuméricos (por ejemplo, !, $, #, %)

oVigencia máxima de la contraseña 180 días

oForzar el historial de contraseña: 5 contraseñas recordadas

oNo contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos.

Se recomienda que tras varios intentos fallidos consecutivos de autenticarse ante el mismo sistema, la cuenta de usuario será bloqueada, al menos, temporalmente y podrá ser habilitada nuevamente por un administrador del sistema. Este hecho se notificará, y quedará registrado, como una incidencia de seguridad.

Los identificadores y claves de acceso asignados a cada usuario son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que puedan derivarse del mal uso, divulgación o pérdida de los mismos.

Durante el tiempo que estén vigentes las contraseñas, si se almacenan, deberá hacerse de manera ininteligible y cifrada, de forma que sea imposible su desciframiento al resto de usuarios.

Debe permanecer deshabilitada, en todas las aplicaciones (aplicaciones de gestión, navegadores, web, etc…), la posibilidad de recordar los datos de acceso; identificadores de usuario, contraseñas de acceso, etc…

6.3 SEGURIDAD EN LA EXPLOTACIÓN

6.3.1 Gestión de activos

Cada responsable administrador de sistemas de información mantiene inventario de los activos que maneja. Según se relaciona en los diferentes procedimientos de su competencia de la ISO 9001 del CSIRC.

La estructura de la red y los sistemas está pensada para evitar fallos ocasionados por código dañino.

6.3.2 Gestión de cambios

Para los cambios, cuando la instalación de actualizaciones y de parches puede impactar en los sistemas, se evalúan y planifican las actualizaciones que se van a realizar, avisando a los usuarios si se van a realizar paradas de algún servicio. Para cambios de cierta relevancia o implantación de nuevos sistemas, se evaluará y planificará el cambio diseñando la estrategia para recuperar el sistema al estado anterior en caso de fallo. Se informa a los afectados de las tareas a realizar y de las acciones que tuvieran que realizar. Se hacen pruebas en un entorno aislado antes del paso a producción, se ejecuta el cambio y tras la correcta finalización se comunica a las partes interesadas.

Si al ejecutar el cambio en producción se produjera un fallo, recuperar la copia de seguridad realizada previa a los cambios llevados a cabo.

6.3.3 Gestión de incidencias

La gestión de incidencias se gestiona principalmente con la herramienta-aplicación **GIA** (Gestión de Incidencias y Averías), y se rige por lo dispuesto en los procedimientos implicados (de la ISO 9001 del CSIRC) que los referencian. Además, se diferenciarán los incidentes de seguridad o ciberincidentes, entendiéndose por incidente de seguridad un suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información, para lo cual se seguirá lo descrito en el procedimiento **PS07 Gestión de Ciberincidentes**.

6.3.4 Gestión de la actividad de los usuarios

En los sistemas que lo permiten, se registra y controla la actividad de los usuarios mediante los **logs** (ficheros o tablas de registros de acceso a sistemas/aplicaciones/datos y/o de su modificación).

El acceso a estos logs está restringido a los administradores de los sistemas. Se detalla en los procedimientos siguientes de la ISO 9001 del CSIRC:

- ***<PE02-17-PSRC: Gestión de los servicios de redes de comunicaciones de UGR>***
- ***<PE02-21-GASR: Gestión, administración y soporte de la red UGR>***
- ***<PE02-22-GSRA: Gestión y administración de sistemas y redes de almacenamiento y despliegue de servicios TIC>***
- ***<PE02-24-BBDD: Administración y gestión de sistemas de bases de datos corporativos>***
- ***<PE02-05-DIAP: Diseño, desarrollo, mantenimiento y administración de aplicaciones informáticas>***

6.3.5 Protección de las claves criptográficas

La gestión de las claves criptográficas se rige por lo dispuesto en la Resolución del Rectorado de la Universidad de Granada, de 8 de octubre de 2012, sobre la **Gestión de Certificados de Sede Electrónica, Certificados de Sello Electrónico y Certificados de Empleado Público**.

En el marco de esta Resolución, la UGR ofrece al público servicios de certificación, de acuerdo con los principios de objetividad, transparencia y no discriminación, emitiendo certificados de la FNMT-RCM bajo la denominación de certificados digitales-firma electrónica- FNMT clase 2 CA.

Estos certificados se rigen por la Declaración de prácticas de certificación, documento de la FNMT, donde se encuentran las condiciones bajo las cuales se prestan los servicios de Certificación.

6.4 MONITORIZACIÓN DEL SISTEMA

Para controlar el tráfico y detectar intentos de intrusión se dispone de diversas herramientas cuyo uso se recoge en los procedimientos siguientes de la ISO 9001 del CSIRC:

- ***<PE02-21-GASR: Gestión, administración y soporte de la red UGR>***
- ***<PE02-17-PSRC: Gestión de los servicios de redes de comunicaciones de UGR>***
- ***<PE02-22-GSRA: Gestión y administración de sistemas y redes de almacenamiento y despliegue de servicios TIC>***

6.5 PROTECCIÓN DE LAS COMUNICACIONES

Cuando las comunicaciones discurren por redes fuera del dominio de seguridad, se utilizan redes privadas virtuales para proteger la integridad, confidencialidad y autenticidad, según se detalla en los procedimientos siguientes de la ISO9001 del CSIRC:

- ***<PE02-21-GASR: Gestión, administración y soporte de la red UGR>***
- ***<PE02-17-PSRC: Gestión de los servicios de redes de comunicaciones de UGR>***
- ***<PE02-22-GSRA: Gestión y administración de sistemas y redes de almacenamiento y despliegue de servicios TIC>***

6.6 PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS

El desarrollo y puesta en servicio del software se rige por lo estipulado en los siguientes procedimientos de la ISO 9001 del CSIRC:

- ***<PE02-05-DIAP: Diseño, desarrollo, mantenimiento y administración de aplicaciones informáticas>***
- ***<PE02-04-PDS: Distribución de software>*** (licencias de explotación y uso)
  - ***<PE02-22-GSRA: Gestión y administración de sistemas y redes de almacenamiento y despliegue de servicios TIC>***
  - ***<PE02-24-BBDD: Administración y gestión de sistemas de bases de datos corporativos>***
- ***<PE02-12-GERA: Gestión de la red administrativa>***

6.7 PROTECCIÓN DE LOS SERVICIOS

Para proteger adecuadamente los servicios se han tomado las medidas oportunas y se recogen en procedimientos de la ISO 9001 del CSIRC.

- Para el correo electrónico:
  - ***<PE02-27-CCII: Gestión de cuentas institucionales>***
- Para los servicios y aplicaciones web:
  - ***<PE02-21-GASR: Gestión, administración y soporte de la red UGR>***
  - ***<PE02-22-GSRA: Gestión y administración de sistemas y redes de almacenamiento y despliegue de servicios TIC>***
  - ***<PE02-24-BBDD: Administración y gestión de sistemas de bases de datos corporativos>***

La denegación de servicio se evita mediante la planificación de la capacidad (ver punto Gestión de la capacidad) y el uso de los sistemas de monitorización.

7 REGISTROS

Se consideran registros correspondientes a este procedimiento:

- Análisis de Riesgos

- Mapas de redes
- Plan de Capacidad
- Contratos y Acuerdos de Nivel de Servicio
- Logs de accesos a los sistemas
- Inventario de activos
- Planes de mantenimiento
- Registros de cambios
- Registros de mantenimiento
- Logs de actividad de los usuarios
- Logs de los sistemas de monitorización
- GIA (Gestión de Incidencias y Averías)

Estos registros son controlados por el Responsable del SGSI durante 3 años.

8 ANEXOS.

No se especifican anexos para este procedimiento.