Título: PROCEDIMIENTO GENERAL DE MEDIDAS DE SEGURIDAD SOBRE LOS DOCUMENTOS Y REGISTROS CONFIDENCIALES DE OCA CERT

Fecha: Enero 2017

ESCRITO POR:

RRHH/INFORMÁTICA

APROBADO POR: DIRECCIÓN GENERAL

DISTRIBUIDO POR: Director Calidad

ÍNDICE:

PROCEDIMIENTO GENERAL DE MEDIDAS DE SEGURIDAD SOBRE LOS DOCUMENTOS Y REGISTROS CONFIDENCIALES DE OCA CERT

1. OBJETIVO

Definir la sistemática llevada a cabo por OCA CERT, en concreto el departamento informática, al respecto de los procesos establecidos para asegurar la gestión de la información confidencial, obtenida o generada durante el desempeño de las actividades de certificación.
.

2. ALCANCE

Todos los empleados de OCA CERT.

3. DEFINICIONES

---

4. METODOLOGÍA

Medidas de seguridad implantadas por OCA Instituto de Certificación, S.L.U. en los contratos de prestación de servicios con acceso a datos

Los siguientes puntos exponen los objetivos de control establecidos en OCA Instituto de Certificación, S.L.U. (en adelante "OCA CERT") como tratante de información confidencial y de datos de carácter personal del Cliente, en garantía del cumplimiento de lo dispuesto en el Reglamento de Medidas de Seguridad de los ficheros que contengan datos de carácter personal (Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal) y los acuerdos de confidencialidad establecidos con el Cliente:

1. **Funciones y obligaciones del personal**
    a. Los trabajadores de OCA CERT tienen firmado el documento "Obligaciones de todos los empleados que traten datos personales" donde están definidas las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información.
    b. Los proveedores y colaboradores de OCA CERT tienen firmado contrato de encargado de tratamiento donde se regula el acceso a los datos y se les impone las medidas de seguridad que deben de cumplir de acuerdo con la legislación y los acuerdos fijados con el cliente de OCA CERT.
    c. Las funciones y obligaciones del personal se encuentran también detalladas en el Documento de Seguridad.
2. **Documento de Seguridad**
    a. OCA CERT tiene desarrollado y actualizado un Documento de Seguridad donde se recogen todas las medidas de índole técnica y organizativas.

3. **Incidencias**
    a. El documento de seguridad tiene descrito el proceso de gestión de incidencias y contiene su registro.
4. **Control de acceso**
    a. Está implantado un Active Directory donde se detallan los privilegios de acceso de cada usuario al sistema de información de OCA CERT.
    b. El Active Directory permite mantener una relación actualizada de los usuarios que tiene acceso a los datos.
    c. El acceso físico al CPD de OCA CERT está estrictamente limitado a personal IT autorizado y mediante identificación personal.
5. **Identificación/autenticación**
    a. El mecanismo de autenticación al sistema de información está basado en nombre de usuario y contraseña.
    b. Está establecida una política de seguridad en las contraseñas, que obliga a los usuarios a cambiarla en un periodo de tiempo establecido.
6. **Copias de seguridad**
    a. Existe un procedimiento de copias de seguridad y de recuperación de datos
    b. Mediante un robot de Backup, se realizan copias de seguridad diarias, tanto de la información corporativa, como de los sistemas y estado de los mismos.
    c. Existe un proceso de recuperación de la información, tanto en caso de pèrdida de datos por parte de un empleado, así como en los casos en los que se precise de la recuperación de sistemas o volcado de datos.
    d. Se verifica periódicamente la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
7. **Soportes y documentos**
    a. Los soportes que contienen datos están debidamente inventariados.
    b. La salida de soportes o documentos que contengan datos confidenciales o personales está debidamente autorizada.
    c. Siempre que se desecha cualquier documento o soporte que contenga datos confidenciales o de carácter personal se procede a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
8. **Almacén de la documentación en papel**
    a. Las áreas o los dispositivos de almacenamiento que contienen documentación confidencial o de carácter personal disponen de mecanismos que obstaculizan su apertura y se encuentran cerrados con llave.
9. **Destrucción de la documentación en papel**
    a. La destrucción de la documentación en papel se realiza mediante destructora de papel o por un método que no permiten su recuperación posterior.

5. ANEXOS

No aplica