POLÍTICA SOBRE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN, Y LA CLASIFICACIÓN DE LA INFORMACIÓN

La información es uno de los activos principales de cualquier empresa y como tal tenemos que protegerla adecuadamente.

Los activos de información pueden estar en formato digital o en otros soportes (papel, película fotográfica, etc.). En formato digital podrán ser desde ficheros de todo tipo (texto, imagen, multimedia, bases de datos,…), pasando por los programas y aplicativos que los utilizan y gestionan, hasta los equipos y sistemas que soportan estos servicios.

Para aplicar las medidas de seguridad ajustadas a cada activo de información debemos realizar un inventario y clasificarlos, de acuerdo con el impacto que ocasionaría su pérdida, difusión, acceso no autorizado, destrucción o alteración, aplicando para ello criterios de confidencialidad, integridad y disponibilidad. Así sabremos qué información debemos cifrar, quién puede utilizarla, quién es responsable de su seguridad, cada cuanto hacer *backup*, etc.

A continuación se realiza un recogido de las principales fuentes de almacenamiento y tratamiento de la información usada para la actividad de RENTAT CISTERNES CTW S.L y se detallan las políticas y buenas prácticas a seguir.

1. ALMACENAMIENTO DE INFORMACIÓN EMPRESARIAL

1.1 ALMACENAMIENTO EN LA RED CORPORATIVA:

En **RENTAT CISTERNES CTW S.L**, para poder disponer de un lugar común de trabajo donde almacenar el resultado de los trabajos individuales y poder compartir información entre los diferentes usuarios de la empresa se dispone de servidores de almacenamiento en red.

En la red corporativa es necesario distinguir entre información general de la empresa que deben utilizar todos los usuarios, e información individual de trabajo de los empleados almacenada en esta red corporativa. Los controles de acceso a esta información son definidos por la dirección y el responsable de sistemas, con el objetivo de limitar quién puede acceder y a dónde.

El contenido de la información almacenada se determina a través de un inventario de la información que debe cubrir al menos los siguientes aspectos: tipo de información almacenada, momento de su almacenamiento y ubicación dentro de los directorios del sistema. Se prestará especial atención cuando la información haya sido catalogada como confidencial o restringida, o si está sujeta a algún requisito legal. Los criterios a seguir para realizar este tipo de clasificación serán contemplados en el punto 6 de este mismo documento.

En el Documento Clasificación información se realiza un inventario de la información, y se pone en conocimiento cuáles son los apartados de almacenamiento disponibles en la red corporativa, la información que se comparte, qué datos deben ser almacenados en los mismos y las responsabilidades que conlleva. Esto se deberá reflejar en la formación de los nuevos empleados y refrescarse cada cierto tiempo.

La Red Corporativa de **RENTAT CISTERNES CTW S.L** está especialmente destinada a su uso empresarial, por ello para poder hacer uso de ella hay que seguir los siguientes criterios:

- La Red Corporativa de **RENTAT CISTERNES CTW S.L** está destinada para usar en el puesto de trabajo con fines empresariales, por ello queda totalmente prohibido el almacenamiento de datos personales o que no sean para desarrollar la actividad laboral. Esta es solo accesible desde los dispositivos permitidos, según los permisos de acceso pertinentes según el perfil del empleado.
- La creación, modificación, actualización o eliminación de las diferentes redes corporativas e información almacenada en ellas, es tarea del personal externalizado y de la persona responsable dentro de la empresa.
- El empleado debe conocer y cumplir la Política de clasificación de la información a la hora de almacenar y eliminar información en la red corporativa. De esta forma se almacenará en la forma y lugar correctos.
- Se ejecutará el plan de copias de seguridad en el que se detalla la información a guardar, cada cuánto tiempo se va a realizar, dónde se va a almacenar y el tiempo de conservación de cada copia.
- Según la política de clasificación de la información, cifraremos la información crítica que se almacene en la red corporativa.

1.2 ALMACENAMIENTO EN LOS EQUIPOS DE TRABAJO

En el puesto de trabajo los empleados utilizan como herramienta equipos informáticos: ordenadores, teléfonos móviles, etc. Estos también generan y transmiten información necesaria para el desempeño de sus funciones. Esta información a veces se almacena de manera local en los discos duros de estos equipos, por lo que surge la necesidad de establecer una serie de procedimientos a seguir para garantizar la correcta conservación de la información y que no peligre su integridad:

- Los equipos físicos de almacenamiento de información de la entidad están destinados para usar en el puesto de trabajo con fines empresariales, por ello queda totalmente prohibido el almacenamiento de datos personales o que no sean para desarrollar la actividad laboral.
- A pesar de la facilidad en la búsqueda de información dentro de un equipo de almacenamiento digital, se recomienda la creación de carpetas dentro del árbol de directorios del equipo para garantizar una accesibilidad óptima para cualquier persona que deba hacer uso del equipo.
- Los discos locales (USB, Discos duros externos o internos, Memorias SSD) cuentan con gran capacidad para almacenar información, pero para evitar problemas de capacidad o de perdida de información por antigüedad o deterioro del dispositivo, se establece un periodo máximo de conservación de la información en este tipo de dispositivos. Transcurrido este tiempo, según la información en cuestión, tendremos que decidir si se transfiere a los servidores empresariales o si se elimina definitivamente. El tiempo transcurrido y la forma de mantener estos activos se recoge en el apartado de Mantenimiento Proactivo dentro del Libro Excel **Activos TIC y riesgos.** Una vez transferida esta información, se deberá de verificar que no se duplique la información en diferentes medios.

1.3 ALMACENAMIENTO EN LA NUBE

El almacenamiento en la nube es una de las formas más óptimas para almacenar información de todo tipo debido a sus características:

- Acceder a la información desde cualquier dispositivo y lugar
- Ahorro de recursos y ahorro económico
- Realización de copias de seguridad de una forma externa, así asegurándonos no perder la información en caso de que se produzca un fallo interno en la empresa.
- Proporciona directorios compartidos con distintos permisos de acceso
- y permite el trabajo colaborativo sobre un documento.

Pero antes de su implantación en la empresa también deben valorarse sus aspectos negativos como la dependencia de terceros o la necesidad de conexión a internet para tener acceso a la información.

Para hacer uso de este tipo de almacenamiento, se deberán de seguir las siguientes directrices:

- El uso de servicios de almacenamiento en nubes públicas solo se puede destinar para almacenar información que esté clasificada de pública.
- En caso de requerir del uso de servicios de almacenamiento en la nube, se elaborará y difundirá una lista de los servicios de almacenamiento en *cloud* permitidos y prohibidos.
- La creación, modificación, actualización o eliminación de los diferentes apartados será responsabilidad del personal externalizado de servicios informáticos, o de la persona interna de la empresa dedicada a los servicios informáticos.

2. APLICACIONES PERMITIDAS

Las normas de protección de la propiedad intelectual obligan a las empresas a usar en todo momento software legal. El uso de software pirata o adquirido de forma fraudulenta podría conllevar sanciones económicas y penales. Además, la instalación y uso de software ilegal en algún dispositivo incrementa los riesgos de infección por malware.

Por otra parte, para evitar fugas de información y garantizar la privacidad de los datos de carácter personal y empresarial, la empresa debe determinar y controlar qué software está autorizado para el tratamiento de la información dentro de la empresa.
Cualquier incidente de seguridad puede repercutir en la imagen de la compañía.

La competencia para la instalación, actualización y borrado es aconsejable únicamente para el personal externo dedicado a los servicios informáticos de **RENTAT CISTERNES CTW S.L** En ningún caso debe permitirse la instalación ni la actualización de software a través de enlaces de webs o correos cuyo origen no sea completamente seguro. Además de ser legal, el software instalado en los equipos debe estar correctamente actualizado.

Se harán conocer las posibles sanciones disciplinarias por el uso de software ilegal o no autorizado en el documento **RECLAMACIONES y REGIMEN DISCIPLINARIO**. Además, la organización se reserva el derecho de auditar o inspeccionar en cualquier momento los equipos de los usuarios para verificar que se cumple esta política.

3. HARDWARE PERMITIDO

Los activos físicos usados por RENTAT CISTERNES CTW S.L serán clasificados en el **Documento _Activos**, donde se detallará el tipo de activo, modelo o versión, número de licencia, localización y sus usuarios.

Para garantizar la mayor seguridad en la actividad empresarial solo serán permitidos los dispositivos adquiridos de fuentes fiables y autorizadas.

Se harán conocer las posibles sanciones disciplinarias por el uso de hardware no autorizado en el documento **PR-RECLAMACIONES y REGIMEN DISCIPLINARIO**.

4. RELACIÓN CON PROVEEDORES Y CLIENTES

Para la posible ejecución de la actividad empresarial de **RENTAT CISTERNES CTW S.L** se requiere de la contratación de proveedores y clientes con los cuales se trabaja conjuntamente para lograr los mejores resultados, con estos actores se comparte información y de nada sirve asegurar al máximo nuestros sistemas si no exigimos la misma seguridad a los proveedores externos que puedan gestionar parte de nuestra información.
Para garantizar la total seguridad de la información que se transfiera durante la actividad empresarial, se exigirá a estos mismos que acaten las políticas recogidas en este documento con la petición de instar a ser respetada -Influenciando .

5. CUMPLIMIENTO LEGAL

Se define la legislación sujeta a la información y las Tecnologías de la Información en el Documento **"_INFORME DE NORMATIVA Y LEGISLACIÓN_TRANSPORTE-SEGURIDAD-RSE".**

6. CLASIFICACIÓN DE LA INFORMACIÓN

Los diferentes documentos que puedan contener información referente a la actividad empresarial de RENTAT CISTERNES CTW S.L deberán ser clasificados según ciertos criterios establecidos. Estos estarán relacionados con las medidas de seguridad que requiera cada tipo de documento debido a sus características.

Esta clasificación se realizará teniendo en cuenta los siguientes criterios:

- **Por su utilidad o funcionalidad:**

- Información de clientes y proveedores.
- Información de compras y ventas.
- Información de personal y gestión interna.
- Información sobre pedidos y procesos de almacén.

- **Por el impacto por robo, borrado o pérdida:**
  - Daño de imagen.
  - Consecuencias legales.
  - Consecuencias económicas.
  - Paralización de la actividad.

Dependiendo de la información que contengan los documentos, podrán clasificarse bajo las siguientes etiquetas:

Pública	Accesible públicamente.
Interna	Accesible solo al personal de la empresa.
Restringida	Para niveles medios de confidencialidad.
Confidencial	Accesible solo por la dirección o personal concreto.

Una vez identificado el grado de clasificación de cada documento, o grupos de documentos, se establecerán las herramientas empleadas para garantizar su seguridad. Estas herramientas pueden ser las siguientes:

- Limitar el acceso a las personas o grupos correspondientes.
  - Archivos físicos: dependiendo del grado de confidencialidad se podrán encontrar en libre acceso en las oficinas de RENTAT CISTERNES CTW S.L, o bajo llave conforme su clasificación se vaya restringiendo.
  - Archivos digitales: los empleados de RENTAT CISTERNES CTW S.L solo tendrán acceso a las carpetas que les sean necesarias para su actividad laboral.
  - Conversaciones verbales: dependiendo del grado de confidencialidad de la conversación se llevará a cabo en un despacho aparte, o no.
- Cifrar la información: la información enviada o recibida por la gestoría será cifrada.
- Realizar copias de seguridad: se realizarán copias de seguridad de la información almacenada a diario para garantizar el correcto guardado de los documentos. Para algunos documentos físicos se realizará una copia en formato digital, y se almacenará de las dos formas.
- Información sujeta a acuerdos de confidencialidad concretos: otras formas de proteger la información en caso de que sea requiero por clientes o proveedores.

La clasificación de la información empresarial, y las herramientas empleadas para garantizar su seguridad serán comprobadas anualmente

Lluis Giralt.
(Dirección)
RENTAT CISTERNES CTW S.L

Motivo de edición: revisión de política basada en evaluación SQAS 2022 (a partir 3 de enero de 2022).