



31

Madrid, 4, 5 y 6 de noviembre 2009

conferencia internacional
de autoridades de protección
de datos y privacidad

Presentación de la Guía de Protección de Datos en las relaciones laborales

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



GUÍA

La protección
de datos en las
relaciones laborales

Agustín Puente Escobar

Abogado del Estado – Jefe del Gabinete Jurídico

José López Calvo

Subdirector General de Inspección de Datos

Agencia Española de Protección de Datos

PRIVACIDAD:
HOY ES
MAÑANA

1	PRESENTACIÓN
2	CUESTIONES GENERALES
2	■ SUPUESTOS DE NO APLICACIÓN DE LA LOPD
3	■ INSCRIPCIÓN DE FICHEROS
6	■ CRITERIOS DE CANCELACIÓN Y BLOQUEO DE LOS DATOS
8	RECURSOS HUMANOS.
8	■ INFORMACIÓN SOBRE EL TRATAMIENTO DE LOS DATOS PERSONALES. MODALIDADES:
9	■ En procedimientos de selección de personal
10	■ En la contratación
11	■ Durante el desarrollo de la prestación laboral
11	■ En las relaciones con los representantes sindicales
12	■ CONSIDERACIÓN DE LOS DATOS ESPECIALMENTE PROTEGIDOS
13	■ SISTEMAS INTERNOS DE DENUNCIAS O "WHISTLEBLOWING"
16	■ CONTRATACIÓN DE SEGUROS DE VIDA Y PLANES DE PENSIONES
18	■ EXTERNALIZACIÓN DE LA GESTIÓN DE LAS NÓMINAS
20	LA PREVENCIÓN DE RIESGOS LABORALES
20	■ El consentimiento en la prevención de riesgos
21	■ Los protagonistas de la prevención de riesgos
23	■ El acceso a los datos por la empresa y los delegados de prevención
26	CONTROLES EMPRESARIALES
26	■ Controles basados en el uso de tecnologías de la información
29	■ Controles sobre el absentismo laboral
32	RELACIONES CON LOS SINDICATOS. COMUNICACIONES DE DATOS, TABLONES, CENSOS.
32	■ Publicaciones de datos personales en tablones
34	■ Cesiones de datos personales a los sindicatos
36	■ Cesiones de datos contenidos en documentos TC2
38	■ Entrega de TC2 al comité de empresa
39	■ Cesión de nóminas y TC2 de los trabajadores de subcontratas a las empresas contratistas
41	DEBERES DE LOS TRABAJADORES QUE ACCEDEN A DATOS PERSONALES: SECRETO Y SEGURIDAD
44	RECURSOS DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

I. Algunas cuestiones previas

- Aplicabilidad de las normas de protección de datos personales
 - Exclusiones subjetivas RLOPD
 - Fichero y tratamiento
- Obligaciones generales del empresario
- Conservación y cancelación de la información

a) Ámbito subjetivo de aplicación de la LOPD

- Criterios de aplicación de los artículos 2.2 y 2.3 RDLOPD.
 - Especial importancia de la finalidad del tratamiento
 - Limitación de los datos en el artículo 2.2
 - La exclusión no opera si la LOPD sólo es aplicable a algunos datos
 - No opera en la aplicación de otras leyes (LGT, LSSI)
- Consecuencias
 - En el entorno de las relaciones laborales o empresario-empleado no operarán las excepciones
 - Los ficheros “de contacto” son productos del fichero de empleados

a) Ámbito objetivo de aplicación de la LOPD

- Aplicación a todo tratamiento total o parcialmente automatizado y a todo fichero no automatizado
- Concepto de fichero
 - Complejidad: el concepto jurídico de fichero puede no coincidir con el de “base de datos”
 - Conjunto estructurado de datos
 - Necesidad de que exista una “lógica organizativa”. Finalidades conexas
 - No es necesario que exista una sola ubicación del fichero
 - Posibles productos o extractos del fichero
- En el ámbito de las relaciones empresa-empleado existirá, en general, un solo fichero con múltiples finalidades

b) Obligaciones generales del empresario

- En relación con los empleados
 - Respeto de los principios
 - Calidad de datos
 - Legitimación para el tratamiento, cesión o transferencia
 - Información a los interesados
 - Atención al ejercicio de los derechos ARCO
- En relación con el fichero o tratamiento
 - Notificación
 - Incluso en caso de externalización
 - Modelos normalizados en el sistema NOTA
 - Seguridad
 - Secreto
 - Conservación y bloqueo de los datos

c) Conservación y bloqueo

- Principios generales

- Conservación ajustada a la finalidad
- La cancelación dará lugar al bloqueo de los datos, quedando únicamente a disposición de las autoridades judiciales o administrativas

- Consecuencias

- Delimitación del período de conservación ajustado a la finalidad
- Delimitación, caso por caso, de los períodos de bloqueo atendiendo a la finalidad y naturaleza del tratamiento y de los datos
- Disponibilidad de los datos únicamente en caso de requerimiento desde el exterior. Inaccesibilidad por los usuarios

2. Tratamiento en la relación laboral

- Especial trascendencia de la aplicación de:
 - Los principios de calidad de datos
 - La legitimación para tratar los datos
 - La información al interesado
- Legitimación para el tratamiento
 - Regla general: vinculación a la relación laboral o mercantil que une a la empresa con el empleado
 - No será necesario recabar el consentimiento, pero
 - El tratamiento deberá ser adecuado al vínculo generado o que pretenda generarse
 - Los datos serán únicamente los necesarios para el desarrollo de ese vínculo
 - El tratamiento de los datos para otros fines sí requerirá consentimiento
 - Deberán tenerse en cuenta las normas especiales (LSSI)

Importancia del deber de información

- El tratamiento de los datos de los empleados puede llevarse a cabo para diversos fines
 - Fácilmente vinculados con el contrato que les une con la empresa
 - Derivados de la organización interna o las políticas del Grupo
 - Decisiones de la matriz sobre retribuciones
 - Existencia de directorios de empleados en el Grupo
 - Sistemas de control del desempeño (videovigilancia, grabaciones)
 - Sistemas de denuncia (whistleblowing)
- Para que el tratamiento sea lícito, aún basado en la relación empresa-empleado será necesario que se informe claramente de estos tratamientos

Supuestos de recogida de datos

- En la selección del personal
 - Criterios generales de Información
 - Establecimiento de procedimientos estándar de entrega de CV con cláusula informativa
 - Establecimiento de sistemas de respuesta e información en caso de presentación “espontánea” del CV
 - Algunas especialidades
 - Procedimientos de selección
 - Información en la convocatoria pública
 - Información acerca de posibles cesiones a otras empresas, sean o no del Grupo
 - Realización de procedimientos de selección por un tercero
 - Naturaleza de responsable o encargado (vínculo con el afectado)
 - Posible conservación de los CV y uso en otros procesos

Supuestos de recogida de datos

- En la contratación y en el desarrollo de la relación empresa-empleado
 - Reglas sobre legitimación para el tratamiento
 - El contrato laboral o mercantil no es el lugar idóneo para solicitar el consentimiento del empleado para el tratamiento de sus datos para fines no vinculados con la relación que le une con el empresario
 - Posibles addendas o anexos
 - Solicitud posterior del consentimiento (expreso o “tácito”)
 - Si surgen nuevos tratamientos vinculados a la relación será necesario informar a los empleados y que conste que los mismos conocen la existencia de estos tratamiento
 - Los controles pueden ser lícitos siempre que exista esa información
 - Importancia de la información a los representantes de los trabajadores

Supuestos de recogida de datos

- Datos especialmente protegidos
 - Proporcionalidad: la recogida debe ser excepcional. Supuestos
 - Afiliación sindical
 - Salud: salud laboral, contingencias, determinados beneficios
 - Origen racial: en circunstancias excepcionales
 - Limitación de finalidad
 - En ocasiones es posible apreciar compatibilidad (Ej.: Comunicación a sindicatos en caso de procedimiento disciplinario)
 - Legitimación
 - Consentimiento expreso o, en algunos casos, habilitación legal
 - Prueba del consentimiento y la información
 - Derecho del afectado a no manifestar determinados datos
 - Seguridad
 - Nivel alto
 - Algunos supuestos especiales (81.5 y 6 RLOPD)

3. Algunos tratamientos especiales

- Sistemas de denuncias o “whistleblowing”
- Beneficios colectivos a empleados (seguros colectivos y planes de pensiones)
- Acceso a información contenida en los TCI, TC2 y nóminas
- Externalización

a) Sistemas de denuncias o “whistleblowing”

- Legitimación: relación jurídica empleado-empresario
 - Puede habilitar también la cesión “intra-grupo”
- Cuestiones relevantes
 - Información previa al establecimiento de estos sistemas
 - En el contrato o en otros documentos internos
 - Información acerca de las posibles cesiones
 - Proporcionalidad: delimitación de los supuestos en que funcionarán los sistemas (incumplimientos “relevantes”)
 - Exactitud y fiabilidad
 - Sistemas basados en la confidencialidad y no en el anonimato
 - Conservación limitada a la investigación y conservación ulterior
 - Especiales garantías de seguridad y secreto
 - Garantías para
 - El ejercicio de los derechos ARCO
 - El conocimiento por el interesado de la denuncia

b) Beneficios colectivos

- Habituales en el seno de la empresa
 - Seguros colectivos de vida o asistencia sanitaria
 - Planes de pensiones
- Legitimación: relación jurídica empleado-empresario
 - Por constar en el contrato o en el Convenio Colectivo
 - Habilita la cesión a la aseguradora o gestora del plan
- Cuestiones relevantes
 - Información: debe constar claramente como una de las condiciones de la relación empresa-empleado
 - En el contrato o en un Anexo posterior
 - Licitud de la comunicación de información sobre el beneficiario, que deberá ser facilitada por el empleado
 - Proporcionalidad: Cesión inicial por la empresa y relación posterior con el empleado
 - Atención a los derechos del empleado
 - En particular su oposición

c) Acceso a TCI, TC2 y nóminas

- Por parte del Comité de empresa
 - Atribuciones de los órganos de representación: control de la relación laboral
 - Proporcionalidad
 - El acceso será posible en cuanto sea necesario para dicha labor de control y vigilancia
 - Posible ampliación por Convenio Colectivo
 - Limitada a datos adecuados a esa actuación (TCI, contratos, relación nominal del TC2)
 - No a datos de salud de los TC2

c) Acceso a TCI, TC2 y nóminas

- En caso de subcontratación de una obra o servicio (acceso por la contratista datos de la subcontratista)
 - Referidos a situaciones previas a la subcontratación (Art. 42.IET)
 - Basta con obtener el certificado favorable de la Tesorería General de la Seguridad Social
 - No es necesario. Falta proporcionalidad
 - Referidos a los trabajadores que desarrollan la obra o servicio subcontratado durante la subcontratación (Art. 40.2 ET)
 - Responsabilidad solidaria del contratista. Obligación de pago exigible directamente al mismo
 - Habilitación legal para la cesión (el contratista es deudor)
 - Podría incluir los datos de salud (Art. 7.3 LOPD) y de afiliación sindical (Art. 4.2 LOPD)
 - Proporcionalidad:
 - Sólo datos de quienes desarrollen la obra o servicio

d) Externalización de la gestión

- Supuesto habitual
 - En la PYME por una empresa dedicada a la gestión de nóminas y RRHH
 - En los Grupos por una empresa específica creada para este fin
- La entidad externa tiene la condición de encargada del tratamiento
 - Cumplimiento de los deberes de la LOPD y el RLOPD en caso de contratación de un encargado
 - Límites del tratamiento
 - Conservación de los datos posterior al contrato
 - Deber de devolución
 - Subcontratación
 - Posible ejercicio de los derechos ante el encargado
 - Medidas de seguridad

4. Prevención de riesgos laborales

- Sujetos de la prevención: Papel de los servicios de prevención
- Flujos de información. Legitimación
- Otras cuestiones relevantes

a) Naturaleza del servicio de prevención

- Servicio propio: integrado en la empresa
 - Condición de usuario del fichero
 - Responsable del fichero: la propia empresa
 - Limitación de perfiles de usuario: sólo acceso por personal del servicio
- Servicio ajeno:
 - El servicio de prevención será responsable del fichero
 - Doctrina de la Audiencia Nacional
 - Deber de tratamiento y conservación de la historia clínica
 - Intercambio de información empresa-servicio: cesiones de datos
- Servicio mancomunado
 - Aplicación de uno de los criterios anteriores según tenga o no personalidad jurídica propia

b) Flujos de información

- Transmisión por la empresa al servicio de los datos identificativos de los empleados y su puesto de trabajo
 - Cesión de datos amparada en la LOPD en conexión con la LPRL
- Tratamiento de datos de salud por el servicio de prevención
 - Con carácter general, requerirá el consentimiento del empleado
 - Supuestos con habilitación legal (art. 22.1 LPRL)
 - Enumeración
 - Necesidad de evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores
 - Verificación de si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa
 - Previsión legal expresa
 - Cuestiones relevantes
 - Decisión empresarial
 - Debe ser informada por los representantes de los trabajadores
 - Posible incorporación de antecedentes (SAN 24/5/2007)

b) Flujos de información

- Acceso a la información de vigilancia de la salud por el empresario (art. 22.4 LPRL)
 - Resultados: El acceso a la información médica de carácter personal se limitará al personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador
 - Conclusiones: El empresario y las personas u órganos con responsabilidades en materia de prevención serán informados de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo
 - Doctrina AN (SAN 31/I/2008): “(...) no puede, desde luego, identificarse con la remisión íntegra del informe, pues la propia Ley se encarga de definir, en los términos expuestos, lo que ha de entenderse por conclusiones en el sentido de incluir todo lo que resulte relevante para la aptitud del trabajador para el desempeño de su puesto de trabajo, o para la adopción de medidas de prevención.”

b) Flujos de información

- Otros accesos a los datos
 - Autoridad laboral
 - Alcance
 - Resultados de vigilancia de la salud
 - Conclusiones de vigilancia de la salud
 - Accidentes y enfermedades que impliquen una IL superior a un día
 - Proporcionalidad y seguridad
 - En caso de servicio propio la comunicación desde los servicios médicos, nunca a través de otras dependencias del empresario
 - Delegados de prevención
 - Función de vigilancia y control
 - Acceso a la información a disposición de la autoridad laboral (art 36.2 d) LPRL)
 - Aplicación del principio de proporcionalidad (datos relacionados con la gravedad y naturaleza de los daños de salud producidos en el entorno laboral)
 - Deber de secreto
 - Historia clínica laboral
 - Supuestos de acceso a la historia clínica de la LAP y la LCCSNS

c) Otras cuestiones relevantes

- Deber de información
 - Tanto por el empresario como por el servicio de prevención, en su caso
- Deber de seguridad
 - Regla general: datos de salud. Nivel alto
 - Especialidad: A los ficheros de empresario que sólo contengan el dato apto/no apto se les aplican las medidas de seguridad de nivel básico (Art. 81.6 RLOPD)
 - Delimitación de rangos de usuarios
- Proporcionalidad
 - En el acceso a los datos de conclusiones por parte del empresario cuando exijan adoptar alguna medida adicional (puede implicar el conocimiento de un dato de salud)
 - En el acceso a los datos por los delegados de prevención
- Atención a los derechos ARCO

5. Controles empresariales

- Principio general
- Controles basados en el uso de tecnologías de la información
- Controles sobre el absentismo laboral

a) Principio general

El Estatuto de los Trabajadores ha atribuido facultades específicas a la empresa que posibilitan el control del desarrollo de la prestación laboral. El ejercicio de estas facultades comporta en muchas ocasiones tratamientos de datos personales.

“3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.

4. El empresario podrá verificar el estado de enfermedad o accidente del trabajador que sea alegado por éste para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones.” (Art. 20.3 y 4 Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores).

b) Controles basados en el uso de tecnologías de la información

Pueden citarse entre otros, los controles biométricos como la huella digital, la videovigilancia, los controles sobre el ordenador, -como las revisiones, el análisis o la monitorización remota, la indexación de la navegación por Internet, o la revisión y monitorización del correo electrónico y/o del uso de ordenadores-, o los controles sobre la ubicación física del trabajador mediante geolocalización.

La legitimación para el tratamiento deriva de la existencia de la relación contractual y, por tanto, de acuerdo con el art. 6.2 LOPD, no se requiere del consentimiento.

A la hora de decidir adoptar una medida de control que comporte un tratamiento de datos personales debe aplicarse el principio de proporcionalidad.

Debe existir una finalidad que, en este caso, no puede ser otra que la establecida por el art. 20.3 ET de “verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales”.

Debe cumplirse con el deber de información a los trabajadores. Este deber resulta particularmente relevante cuando se trate de controles sobre el uso de Internet y/o del correo electrónico.

Puede ser muy recomendable informar también a los representantes de los trabajadores de las políticas adoptadas en esta materia.

“Es necesario recordar lo que ya se dijo sobre la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial. (...) Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de los medios e informar a los trabajadores de que va existir control.”

(Sentencia de la Sala de lo Social del Tribunal Supremo de 26 de septiembre de 2007.

c) Controles sobre el absentismo laboral

El Estatuto de los Trabajadores faculta a las empresas para realizar controles en los supuestos de enfermedad o accidente de trabajo que motivan faltas de asistencia. Este control se realizará mediante reconocimiento médico.

«4. El empresario podrá verificar el estado de enfermedad o accidente del trabajador que sea alegado por éste para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones. (art. 20 ET)».

Hay que tener en cuenta dos elementos que se han señalado

- El tratamiento de datos de salud requerirá del consentimiento expreso del trabajador. La empresa únicamente puede conocer las condiciones de aptitud.
- La incorporación de datos de salud a un fichero con la única finalidad de realizar controles del absentismo resulta desproporcionada.

Cuando se realiza mediante la contratación de un prestador de servicios, además de cumplir con las obligaciones propias de un encargado del tratamiento, debe atenerse a ciertas condiciones:

La información al trabajador debe ser muy precisa e indicar que se trata de un control laboral. Como indica el art.5 una de las informaciones que deben facilitarse en su caso se refiere a la obligación de facilitar datos y las consecuencias de la negativa a suministrarlos.

La información se referirá a que se esta verificando su condiciones de aptitud por cuenta de la empresa y de la naturaleza de este tratamiento conforme al art. 20.4 del Estatuto de los trabajadores.

No existe obstáculo a que se persiga la doble finalidad de verificar el estado de salud del trabajador y controlar el absentismo. Pero, si existe un tratamiento relacionado con la salud deberá obtenerse el consentimiento expreso del trabajador.

Para este tipo de servicios el prestador externo tiene la condición de encargado del tratamiento y deben de cumplirse las previsiones del artículo 12 de la LOPD.

5. Relaciones con los sindicatos

- Publicación de datos personales en tablones
- Acceso a datos por el Comité de Empresa
- Cesiones de datos personales a sindicatos
- Uso del correo electrónico a efectos sindicales

a) Publicaciones de datos personales en tablones.

Derecho a disponer de un tablón de anuncios que permita facilitar información sindical a los trabajadores.

Cuando documentos contienen datos personales la simple publicación de éstos constituye un tratamiento que puede comportar el acceso a datos por terceros carentes de legitimación.

Deben por ello adoptarse medidas de seguridad que impidan la colocación de datos por terceros (mampara cerrada con llave)

Es fundamental que los tablones sindicales online se sitúen en las intranet de la empresa nunca en Internet.

La información publicada debería limitarse a la estrictamente necesaria. Así, si en un momento dado decidiera publicarse una determinada resolución administrativa o de una sentencia judicial de interés para los trabajadores debería procederse a la anonimización de los datos

b) Acceso a datos por el comité de empresa

En todos aquellos casos en que la información pueda presentarse de modo estadístico o anonimizado permitiendo el comité cumplir con sus funciones se optará por éste método.

El comité de empresa o los representantes sindicales que acceden a información de los trabajadores están obligados a guardar secreto “2. Los miembros del comité de empresa y éste en su conjunto, así como, en su caso, los expertos que les asistan, deberán observar el deber de sigilo...”

Art. 65 del Estatuto de los Trabajadores

c) Cesiones de datos personales a los sindicatos

La cesión de datos más común a las organizaciones sindicales es la relativa al cobro de la cuota sindical en el pago de la nómina.

Es recomendable disponer de procedimientos de captación del consentimiento como impresos o modelos de solicitud en los que el trabajador autorice de modo expreso y por escrito el tratamiento.

Es muy importante limitar el uso de estos datos a la finalidad para la que se han recabado: cobrar la cuota y transferir las cantidades a la organización sindical.

d) Uso correo electrónico a efectos sindicales

El envío de este tipo de mensajes de correo electrónico constituye un derecho de los sindicatos amparado por el derecho fundamental la libertad sindical (STC.281/2005). No obstante deben darse ciertas condiciones como que la empresa disponga del servicio de correo electrónico y que los envíos se realicen de modo proporcional y que no perjudique el normal funcionamiento de la organización.

La utilización de listas de distribución permite que el sindicato remita la información a una dirección corporativa del tipo listasindical@empresa.es, sin acceso a los datos.

En ningún caso se cederán datos como la dirección de cuentas privadas del trabajador.

El sindicato debe satisfacer el derecho de oposición de los trabajadores salvo en el supuesto de elecciones sindicales, momento en el cual prevalece la libertad sindical respecto del derecho a la protección de datos.

7. Deberes de los trabajadores: secreto y seguridad

«El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado (art. 9)

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo (art. 10)».

Para el adecuado cumplimiento de estos dos deberes resulta ineludible disponer de políticas de gestión de personal en los que se definan de modo muy claro los perfiles funcionales de cada puesto.

El abandono de documentos sin destruir en la basura común por el personal de limpieza, es una de las infracciones más comunes en materia de protección de datos. Recientemente la ausencia de límites a la instalación de programas peer to peer, como el conocido e-mule, ha expuesto al acceso de cualquiera miles de datos de los ciudadanos.

En el caso de que se consulten datos telefónicamente el trabajador debe extremar la cautela para comprobar correctamente la identidad de la persona que solicita la información.



31

Madrid, 4, 5 y 6 de noviembre 2009

conferencia internacional
de autoridades de protección
de datos y privacidad

**Muchas gracias
por su atención**

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



GUÍA

La protección
de datos en las
relaciones laborales

PRIVACIDAD:
HOY ES
MAÑANA