IFCT0109. SEGURIDAD INFORMÁTICA

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

UD02

APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. **LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD**
2. DERECHOS DE LOS CIUDADANOS EN LA PROTECCIÓN DE SUS DATOS PERSONALES
3. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: MEDIDAS DE CUMPLIMIENTO EN EL RGPD
4. LA AUDITORÍA DE PROTECCIÓN DE DATOS
5. AUDITORÍA DE SISTEMAS DE INFORMACIÓN

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

VAMOS A ESTUDIAR:

- EL **CONSENTIMIENTO** EN LO QUE RESPECTA A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
- CONOCER CÓMO **REVOCAR EL CONSENTIMIENTO**
- APRENDER **CÓMO Y QUIÉN DEBE INFORMAR**
- RECONOCER LAS **CATEGORÍAS ESPECIALES DE DATOS**.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

EL CONSENTIMIENTO DEL INTERESADO

EL **RGPD** MANTIENE EL **PRINCIPIO** DE QUE **TODO TRATAMIENTO DE DATOS NECESITA APOYARSE EN UNA BASE QUE LO LEGITIME**.

HAY QUE DESTACAR QUE EN ESE SENTIDO EL **RGPD NO IMPLICA CAMBIOS PARA LOS RESPONSABLES DEL TRATAMIENTO DE DATOS**.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

EL CONSENTIMIENTO DEL INTERESADO

VEAMOS EL **CONSENTIMIENTO DEL INTERESADO**.

EL **RGPD**, EN EL ARTÍCULO 4, REFERENTE A LAS **DEFINICIONES**, EN EL APARTADO 11, SOBRE LA **DEFINICIÓN DE CONSENTIMIENTO**, ESTABLECE:

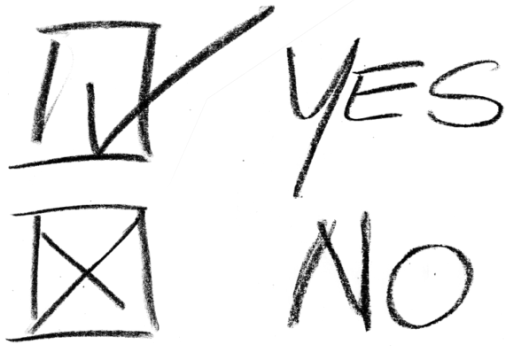
> *"A EFECTOS DEL PRESENTE REGLAMENTO SE ENTENDERÁ POR:*
>
> ***CONSENTIMIENTO DEL INTERESADO: TODA MANIFESTACIÓN DE VOLUNTAD LIBRE, ESPECÍFICA, INFORMADA E INEQUÍVOCA*** *POR LA QUE EL INTERESADO ACEPTA, YA SEA MEDIANTE UNA DECLARACIÓN O UNA CLARA ACCIÓN AFIRMATIVA, EL TRATAMIENTO DE DATOS PERSONALES QUE LE CONCIERNEN"*

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

EL CONSENTIMIENTO DEL INTERESADO

PARA EXPRESAR EL CONSENTIMIENTO, SE PERMITE:

- MEDIANTE UNA DECLARACIÓN
- MEDIANTE UNA ACCIÓN



POR TANTO, **NO VALE EL *CONSENTIMIENTO TÁCITO.***

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

EL CONSENTIMIENTO DEL INTERESADO

¿CÓMO DAR EL CONSENTIMIENTO?

- **MEDIANTE UNA DECLARACIÓN POR ESCRITO**, INCLUSIVE POR MEDIOS ELECTRÓNICOS
- **MEDIANTE UNA DECLARACIÓN VERBAL**

ESTO PODRÁ INCLUIR:

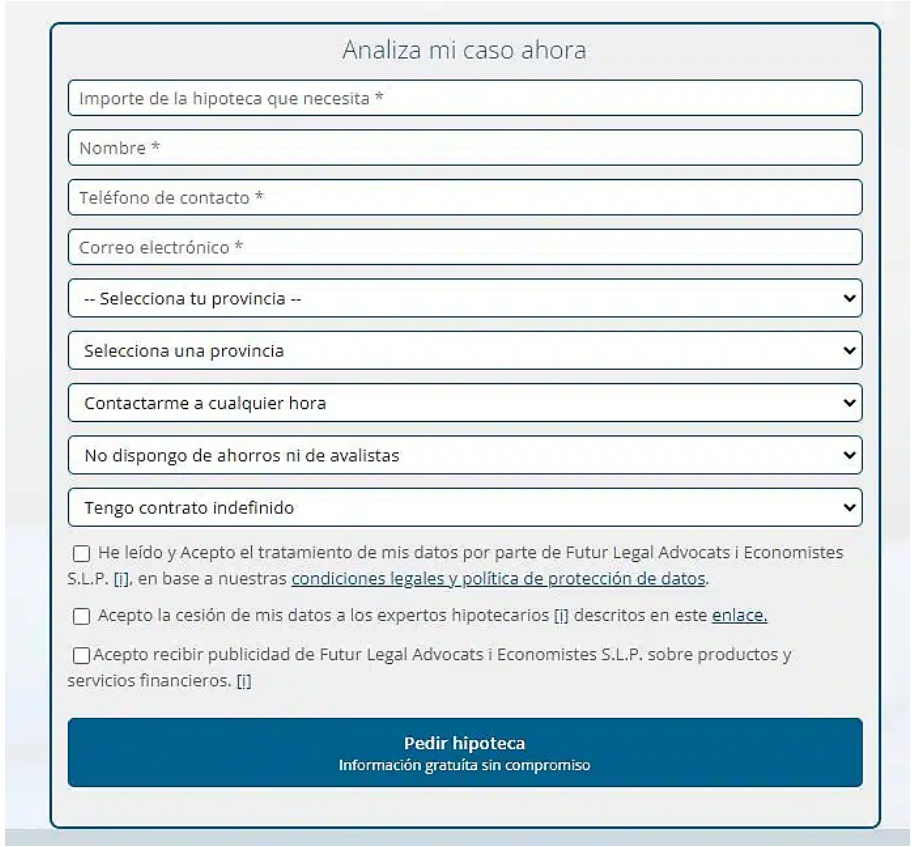
- MARCAR UNA CASILLA DE UN SITIO WEB DE INTERNET
- CUALQUIER OTRA DECLARACIÓN O CONDUCTA QUE INDIQUE CLARAMENTE EN ESTE CONTEXTO QUE EL INTERESADO ACEPTA LA PROPUESTA DE TRATAMIENTO DE SUS DATOS PERSONALES

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

EL CONSENTIMIENTO DEL INTERESADO

LAS **CASILLAS YA MARCADAS**, EL **SILENCIO O** LA **INACCIÓN, NO** CONSTITUYEN CONSENTIMIENTO.

ADEMÁS, DEBERÁ DARSE CONSENTIMIENTO **PARA CADA UNO DE LOS TRATAMIENTOS.**



1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

EL CONSENTIMIENTO DEL INTERESADO

EL RESPONSABLE DEL TRATAMIENTO **DEBE SER CAPAZ DE DEMOSTRAR QUE EL INTERESADO HA DADO SU CONSENTIMIENTO** AL TRATAMIENTO.

PARA ELLO, DEBE PROPORCIONAR UN **MODELO DE DECLARACIÓN DE CONSENTIMIENTO**, QUE SEA **DE FÁCIL ACCESO**, EMPLEE UN **LENGUAJE CLARO Y SENCILLO**, Y QUE **NO CONTENGA CLÁUSULAS ABUSIVAS.**

EL INTERESADO DEBE CONOCER, COMO MÍNIMO**, LA IDENTIDAD DEL RESPONSABLE DEL TRATAMIENTO Y LOS FINES DEL TRATAMIENTO** A LOS CUALES ESTÁN DESTINADOS LOS DATOS PERSONALES.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

EL CONSENTIMIENTO DEL INTERESADO

EL CONSENTIMIENTO **NO SE CONSIDERA LIBREMENTE PRESTADO** CUANDO:

- NO PERMITA AUTORIZAR POR SEPARADO LAS DISTINTAS OPERACIONES DE TRATAMIENTO.
- EL CUMPLIMIENTO DE UN CONTRATO SEA DEPENDIENTE DEL CONSENTIMIENTO, AUN CUANDO ESTE NO SEA NECESARIO PARA DICHO CUMPLIMIENTO.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

EL CONSENTIMIENTO DEL INTERESADO

LA **LOPDGDD** INDICA QUE **NO PUEDE SUPEDITARSE LA EJECUCIÓN DEL CONTRATO A QUE EL AFECTADO CONSIENTA EL TRATAMIENTO DE LOS DATOS PERSONALES** PARA FINALIDADES QUE NO GUARDEN RELACIÓN CON EL MANTENIMIENTO, DESARROLLO O CONTROL DE LA RELACIÓN CONTRACTUAL.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

EL CONSENTIMIENTO DEL INTERESADO

TRATAMIENTO DE DATOS INICIADOS ANTES DEL 25 DE MAYO DE 2018 BASADOS EN UN CONSENTIMIENTO QUE CUMPLE CON LOS REQUISITOS DEL RGPD

NO SERÁ NECESARIO PEDIR QUE EL INTERESADO PRESTE SU CONSENTIMIENTO SI FUERA A SEGUIR EL MISMO FIN PARA EL QUE SE CONSINTIÓ.

BASTARÁ CON UNA COMUNICACIÓN DEL CAMBIO O MODIFICACIÓN DE LA NORMATIVA.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

EL CONSENTIMIENTO DEL INTERESADO

TRATAMIENTO DE DATOS INICIADOS DESPUÉS DEL 25 DE MAYO DE 2018 BASADOS EN UN CONSENTIMIENTO QUE CUMPLE CON LOS REQUISITOS DEL RGPD

SERÁ NECESARIO PEDIR AL INTERESADO SU CONSENTIMIENTO, SI EL TRATAMIENTO DE DATOS PERSIGUIERE UNOS FINES DISTINTOS A LOS INICIALES Y ASÍ, APROVECHAR ESTA SITUACIÓN PARA INFORMAR DE LAS NUEVAS CONDICIONES.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

REVOCACIÓN DEL CONSENTIMIENTO

EL **RGPD**, EN EL ARTÍCULO 7.3 ESTABLECE:

> *"EL INTERESADO **TENDRÁ DERECHO A RETIRAR SU CONSENTIMIENTO EN CUALQUIER MOMENTO.** LA RETIRADA DEL CONSENTIMIENTO NO AFECTARÁ A LA LICITUD DEL TRATAMIENTO BASADA EN EL CONSENTIMIENTO PREVIO A SU RETIRADA. ANTES DE DAR SU CONSENTIMIENTO, EL INTERESADO SERÁ INFORMADO DE ELLO. **SERÁ TAN FÁCIL RETIRAR EL CONSENTIMIENTO COMO DARLO."***

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

REVOCACIÓN DEL CONSENTIMIENTO

CAUSA

EL **RGPD** FACULTA AL INTERESADO A REVOCAR EL CONSENTIMIENTO EN CUALQUIER MOMENTO.

ESTO SE PUEDE REALIZAR A TRAVÉS DE UN MERO ACTO O DECLARACIÓN DE VOLUNTAD, **SIN NECESIDAD DE JUSTIFICAR O PROBAR CAUSA ALGUNA.**

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

REVOCACIÓN DEL CONSENTIMIENTO

IRRETROACTIVIDAD

LA RETIRADA DEL CONSENTIMIENTO NO AFECTARÁ A LA LICITUD DEL TRATAMIENTO BASADA EN EL CONSENTIMIENTO PREVIO A SU RETIRADA.

FACILIDAD

EL RGPD REGULA QUE: "***SERÁ TAN FÁCIL RETIRAR EL CONSENTIMIENTO COMO DARLO***".

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

REVOCACIÓN DEL CONSENTIMIENTO

INFORMACIÓN

EL **RGPD** ESTABLECE QUE **ANTES DE DAR SU CONSENTIMIENTO, EL INTERESADO SERÁ INFORMADO DE ELLOS**.

SE REFIERE NO SOLO "A LA POSIBILIDAD DE LA **REVOCACIÓN O RETIRADA** (EN CUALQUIER MOMENTO) Y SU **IRRETROACTIVIDAD**, O **LICITUD DEL TRATAMIENTO** BASADA EN EL CONSENTIMIENTO PREVIO, SINO TAMBIÉN A **LOS MEDIOS PARA** PODER HACERLO (QUE HAN DE SER FÁCILES Y GRATUITOS)".

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

EL CONSENTIMIENTO INFORMADO

¿QUIÉN DEBE INFORMAR?

LA OBLIGACIÓN DE INFORMAR RECAE SOBRE EL RESPONSABLE DEL TRATAMIENTO, QUE DEBERÁ PONER A DISPOSICIÓN DE LOS SUJETOS INTERESADOS, CUANDO ESTOS SOLICITAREN LOS DATOS PREVIAMENTE A LA RECOGIDA DE LOS DATOS O REGISTRO.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

EL CONSENTIMIENTO INFORMADO

DESAPARECEN LOS CONSENTIMIENTOS TÁCITOS, ÉSTOS DEBERÁN ADAPTARSE A LOS REQUISITOS ESTABLECIDOS POR EL MISMO, DE MANERA QUE DEBE ENCONTRARSE OTRA FORMA DE LEGITIMACIÓN PARA ESTOS TRATAMIENTOS:

- MEDIANTE UNA NUEVA SOLICITUD DE CONSENTIMIENTO ACORDE CON EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS.
- MEDIANTE LA APLICACIÓN DE ALGÚN OTRO SUPUESTO DE LEGITIMACIÓN, COMO PODRÍA SER LA REGLA DEL INTERÉS LEGÍTIMO QUE TENDRÍA QUE PONDERARSE.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

CONSENTIMIENTO DE LOS NIÑOS

EL **RGPD** ESTABLECE QUE LOS MENORES SON LOS QUE TIENEN MENOS DE 16 AÑOS.

ARTÍCULO 8

CONDICIONES APLICABLES AL CONSENTIMIENTO DEL NIÑO EN RELACIÓN CON LOS SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

1. CUANDO SE APLIQUE EL ARTÍCULO 6, APARTADO 1, LETRA A), EN RELACIÓN CON LA OFERTA DIRECTA A NIÑOS DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN, EL TRATAMIENTO DE LOS DATOS PERSONALES DE UN NIÑO SE CONSIDERARÁ LÍCITO CUANDO TENGA COMO MÍNIMO 16 AÑOS. SI EL NIÑO ES MENOR DE 16 AÑOS, TAL TRATAMIENTO ÚNICAMENTE SE CONSIDERARÁ LÍCITO SI EL CONSENTIMIENTO LO DIO O AUTORIZÓ EL TITULAR DE LA PATRIA POTESTAD O TUTELA SOBRE EL NIÑO, Y SOLO EN LA MEDIDA EN QUE SE DIO O AUTORIZÓ.

LOS ESTADOS MIEMBROS PODRÁN ESTABLECER POR LEY UNA EDAD INFERIOR A TALES FINES, SIEMPRE QUE ESTA NO SEA INFERIOR A 13 AÑOS.

2. EL RESPONSABLE DEL TRATAMIENTO HARÁ ESFUERZOS RAZONABLES PARA VERIFICAR EN TALES CASOS QUE EL CONSENTIMIENTO FUE DADO O AUTORIZADO POR EL TITULAR DE LA PATRIA POTESTAD O TUTELA SOBRE EL NIÑO, TENIENDO EN CUENTA LA TECNOLOGÍA DISPONIBLE.

3. EL APARTADO 1 NO AFECTARÁ A LAS DISPOSICIONES GENERALES DEL DERECHO CONTRACTUAL DE LOS ESTADOS MIEMBROS, COMO LAS NORMAS RELATIVAS A LA VALIDEZ, FORMACIÓN O EFECTOS DE LOS CONTRATOS EN RELACIÓN CON UN NIÑO.”

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

CONSENTIMIENTO DE LOS NIÑOS

EN ESPAÑA, LA **LOPDGDD** ESTABLECE QUE LOS MENORES SON LOS QUE TIENEN MENOS DE 14 AÑOS.

ARTÍCULO 7

CONSENTIMIENTO DE LOS MENORES DE EDAD

1. EL TRATAMIENTO DE LOS DATOS PERSONALES DE UN MENOR DE EDAD ÚNICAMENTE PODRÁ FUNDARSE EN SU CONSENTIMIENTO CUANDO SEA MAYOR DE CATORCE AÑOS.

SE EXCEPTÚAN LOS SUPUESTOS EN QUE LA LEY EXIJA LA ASISTENCIA DE LOS TITULARES DE LA PATRIA POTESTAD O TUTELA PARA LA CELEBRACIÓN DEL ACTO O NEGOCIO JURÍDICO EN CUYO CONTEXTO SE RECABA EL CONSENTIMIENTO PARA EL TRATAMIENTO.

2. EL TRATAMIENTO DE LOS DATOS DE LOS MENORES DE CATORCE AÑOS, FUNDADO EN EL CONSENTIMIENTO, SOLO SERÁ LÍCITO SI CONSTA EL DEL TITULAR DE LA PATRIA POTESTAD O TUTELA, CON EL ALCANCE QUE DETERMINEN LOS TITULARES DE LA PATRIA POTESTAD O TUTELA.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

CONSENTIMIENTO DE LOS NIÑOS

EL TRATAMIENTO DE LOS DATOS DE LOS MENORES DE 14 AÑOS, FUNDADO EN EL CONSENTIMIENTO, **SOLO SERÁ LÍCITO SI CONSTA EL DEL TITULAR DE LA PATRIA POTESTAD O TUTELA**.

EL CONSENTIMIENTO DEL TITULAR DE LA PATRIA POTESTAD O TUTELA NO DEBE SER NECESARIO EN EL CONTEXTO DE LOS SERVICIOS PREVENTIVOS O DE ASESORAMIENTO OFRECIDOS DIRECTAMENTE A LOS NIÑOS.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

CONSENTIMIENTO DE LOS NIÑOS

EL **CÓDIGO CIVIL** ESTIPULA QUE **LA PATRIA POTESTAD SE EJERCERÁ POR AMBOS PROGENITORES O POR UNO DE ELLOS CON EL CONSENTIMIENTO EXPRESO O TÁCITO DEL OTRO**, SIENDO VÁLIDOS LOS ACTOS QUE REALICE UNO DE ELLOS CONFORME AL USO SOCIAL Y A LAS CIRCUNSTANCIAS O LAS SITUACIONES DE URGENTE NECESIDAD.

EN CASO DE DESACUERDO, CUALQUIERA DE LOS DOS PODRÁ ACUDIR AL JUEZ, QUIEN DECIDIRÁ AL RESPECTO.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

CONSENTIMIENTO DE LOS NIÑOS

EN EL SUPUESTO DE PADRES SEPARADOS EN EL QUE LA GUARDA Y CUSTODIA DEL HIJO MENOR HA SIDO ATRIBUIDA A UNO DE LOS PROGENITORES, PERO AMBOS CONSERVAN LA PATRIA POTESTAD.

DE NO ALCANZARSE UN ACUERDO HABRÁ DE SOMETERSE LA CUESTIÓN AL JUEZ CORRESPONDIENTE.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

CATEGORÍAS ESPECIALES DE DATOS

LAS CATEGORÍAS ESPECIALES DE DATOS SON AQUELLAS QUE INCLUYEN DATOS QUE REVELEN **EL ORIGEN ÉTNICO O RACIAL, LAS OPINIONES POLÍTICAS, CONVICCIONES RELIGIOSAS O FILOSÓFICAS, AFILIACIÓN SINDICAL, DATOS GENÉTICOS, DATOS BIOMÉTRICOS** DIRIGIDOS A IDENTIFICAR DE MANERA UNÍVOCA A UNA PERSONA FÍSICA, DATOS RELATIVOS A LA **SALUD** O A LA **VIDA SEXUAL O LAS ORIENTACIONES SEXUALES** DE UNA PERSONA FÍSICA.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

CATEGORÍAS ESPECIALES DE DATOS

CUANDO EL TRATAMIENTO *DE CATEGORÍAS ESPECIALES DE DATOS PERSONALES* ***SEA NECESARIO PARA*** *FINES DE MEDICINA PREVENTIVA O LABORAL, EVALUACIÓN DE LA CAPACIDAD LABORAL DEL TRABAJADOR, DIAGNÓSTICO MÉDICO, PRESTACIÓN DE ASISTENCIA O TRATAMIENTO DE TIPO SANITARIO O SOCIAL, O GESTIÓN DE LOS SISTEMAS Y SERVICIOS DE ASISTENCIA SANITARIA Y SOCIAL,* ***LOS DATOS PERSONALES PODRÁN TRATARSE CUANDO SU TRATAMIENTO SEA REALIZADO POR UN PROFESIONAL SUJETO A LA OBLIGACIÓN DE SECRETO PROFESIONAL,*** *O BAJO SU RESPONSABILIDAD, DE ACUERDO CON EL DERECHO DE LA UNIÓN O DE LOS ESTADOS MIEMBROS O CON LAS NORMAS ESTABLECIDAS POR LOS ORGANISMOS NACIONALES COMPETENTES,* ***O POR CUALQUIER OTRA PERSONA SUJETA TAMBIÉN A LA OBLIGACIÓN DE SECRETO*** *DE ACUERDO CON EL DERECHO DE LA UNIÓN O DE LOS ESTADOS MIEMBROS O DE LAS NORMAS ESTABLECIDAS POR LOS ORGANISMOS NACIONALES COMPETENTES.*

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

CATEGORÍAS ESPECIALES DE DATOS

LA **LOPDGDD** HA INTRODUCIDO CIERTAS **RESTRICCIONES AL TRATAMIENTO** DE DATOS BASADO EN EL CONSENTIMIENTO EXPLÍCITO DEL AFECTADO A FIN DE EVITAR SITUACIONES DISCRIMINATORIAS.

EL SOLO CONSENTIMIENTO DEL AFECTADO NO BASTARÁ PARA LEVANTAR LA PROHIBICIÓN DEL TRATAMIENTO DE DATOS CUYA FINALIDAD PRINCIPAL SEA IDENTIFICAR SU IDEOLOGÍA, AFILIACIÓN SINDICAL, RELIGIÓN, ORIENTACIÓN SEXUAL, CREENCIAS U ORIGEN RACIAL O ÉTNICO.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

DATOS RELATIVOS A INFRACCIONES Y CONDENAS PENALES

DENTRO DEL RGPD, EN CONCRETO EN SU ARTÍCULO 10, RECOGE **EL TRATAMIENTO DE DATOS PERSONALES RELATIVOS A CONDENAS E INFRACCIONES PENALES O DE MEDIDAS DE SEGURIDAD CONEXAS**.

ESOS DATOS NO QUEDAN INCORPORADOS A LAS CATEGORÍAS ESPECIALES DE DATOS.

CONTIENE **DOS PREVISIONES**:

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

DATOS RELATIVOS A INFRACCIONES Y CONDENAS PENALES

- SOLO PODRÁ LLEVARSE UN **REGISTRO COMPLETO DE CONDENAS PENALES** BAJO EL CONTROL DE LAS AUTORIDADES PÚBLICAS.
- EL TRATAMIENTO DE DATOS PERSONALES RELATIVOS A CONDENAS E INFRACCIONES PENALES O MEDIDAS DE SEGURIDAD CONEXAS SOBRE LA BASE DEL ARTÍCULO 6, APARTADO 1, **SÓLO PODRÁ LLEVARSE A CABO BAJO LA SUPERVISIÓN DE LAS AUTORIDADES PÚBLICAS O CUANDO LO AUTORICE EL DERECHO DE LA UNIÓN O DE LOS ESTADOS MIEMBROS** QUE ESTABLEZCA GARANTÍAS ADECUADAS PARA LOS DERECHOS Y LIBERTADES DE LOS INTERESADOS.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

DATOS RELATIVOS A INFRACCIONES Y CONDENAS PENALES

ARTÍCULO 10 DEL RGPD

FUERA DE ESTOS SUPUESTOS, EL TRATAMIENTO DE DATOS PERSONALES RELATIVOS A CONDENAS E INFRACCIONES PENALES, ASÍ COMO A PROCEDIMIENTOS Y MEDIDAS CAUTELARES Y DE SEGURIDAD CONEXAS, **SOLO SERÁ POSIBLE CUANDO SEAN LLEVADOS A CABO POR ABOGADOS Y PROCURADORES** Y TENGAN POR OBJETO RECOGER LA INFORMACIÓN FACILITADA POR SUS CLIENTES **PARA EL EJERCICIO DE SUS FUNCIONES**.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

TRATAMIENTO QUE NO REQUIERE IDENTIFICACIÓN

EL **RGPD** CONTEMPLA EXPRESAMENTE LA POSIBLE EXISTENCIA DE **SUPUESTOS EN LOS QUE LOS QUE LOS DATOS PERSONALES NO PERMITEN IDENTIFICAR A UNA PERSONA FÍSICA** Y EN LOS QUE, POR TANTO, **EL RESPONSABLE NO ESTARÍA OBLIGADO A OBTENER INFORMACIÓN ADICIONAL PARA IDENTIFICAR AL INTERESADO** CUANDO TAL IDENTIFICACIÓN ÚNICAMENTE TUVIERA POR OBJETO CUMPLIR CON LAS DISPOSICIONES DEL REGLAMENTO.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

TRATAMIENTO QUE NO REQUIERE IDENTIFICACIÓN

EL CONSIDERANDO 57 SEÑALA QUE, SI LOS DATOS PERSONALES TRATADOS POR UN RESPONSABLE NO LE PERMITEN IDENTIFICAR A UNA PERSONA FÍSICA, **EL RESPONSABLE NO DEBE ESTAR OBLIGADO A OBTENER INFORMACIÓN ADICIONAL PARA IDENTIFICAR AL INTERESADO** CON LA ÚNICA FINALIDAD DE CUMPLIR CUALQUIER DISPOSICIÓN DEL REGLAMENTO.

NO OBSTANTE, **EL RESPONSABLE DEL TRATAMIENTO NO DEBE NEGARSE A RECIBIR INFORMACIÓN ADICIONAL** FACILITADA POR EL INTERESADO A FIN DE RESPALDARLE EN EL EJERCICIO DE SUS DERECHOS.

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD

TRATAMIENTO QUE NO REQUIERE IDENTIFICACIÓN

LOS TRATAMIENTOS DE DATOS QUE NO REQUIEREN IDENTIFICACIÓN SUELEN SER SUPUESTOS MUY USUALES EN LOS QUE **EL RESPONSABLE ÚNICAMENTE CONOCE DEL INTERESADO LAS CREDENCIALES DE ACCESO A LA PLATAFORMA O A LA PROPIA WEB.**

EN ESTOS CASOS ES POSIBLE LIMITAR EL ACCESO A LA WEB A TRAVÉS DEL SISTEMA DE USUARIO Y CONTRASEÑA, NO EXISTIENDO MÉTODO ALGUNO PARA IDENTIFICAR A LA PERSONA QUE ESTÁ DETRÁS DE ESAS CREDENCIALES (POR TANTO, TODA LA ESTADÍSTICA O COMPORTAMIENTO EN LA WEB NO PUEDE SER ATRIBUIBLE A UNA PERSONA FÍSICA IDENTIFICABLE)

CONTENIDOS

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD
2. **DERECHOS DE LOS CIUDADANOS EN LA PROTECCIÓN DE SUS DATOS PERSONALES**
3. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: MEDIDAS DE CUMPLIMIENTO EN EL RGPD
4. LA AUDITORÍA DE PROTECCIÓN DE DATOS
5. AUDITORÍA DE SISTEMAS DE INFORMACIÓN

2. DERECHOS DE LOS CIUDADANOS EN LA PROTECCIÓN DE SUS DATOS PERSONALES

LA NORMATIVA DE PROTECCIÓN DE DATOS PERMITE AL INTERESADO EJERCITAR ANTE EL RESPONSABLE LOS *DERECHOS DE ACCESO, RECTIFICACIÓN, OPOSICIÓN, SUPRESIÓN* ("DERECHO AL OLVIDO"), *LIMITACIÓN DEL TRATAMIENTO, PORTABILIDAD Y NO SER OBJETO DE DECISIONES INDIVIDUALIZADAS*.

DERECHO DE ACCESO

SUPONE EL **DERECHO DEL INTERESADO A DIRIGIRSE AL RESPONSABLE DEL TRATAMIENTO PARA CONOCER SI ESTÁ TRATANDO O NO SUS DATOS** DE CARÁCTER PERSONAL DEL INTERESADO **Y**, EN CASO DE QUE SE ESTÉ REALIZANDO DICHO TRATAMIENTO **OBTENER INFORMACIÓN ADICIONAL.**

2. DERECHOS DE LOS CIUDADANOS EN LA PROTECCIÓN DE SUS DATOS PERSONALES

DERECHO DE RECTIFICACIÓN

SUPONE QUE EL INTERESADO PODRÁ **OBTENER SIN DILACIÓN** INDEBIDA DEL RESPONSABLE DEL TRATAMIENTO **LA RECTIFICACIÓN DE SUS DATOS PERSONALES INEXACTOS**.

DERECHO DE OPOSICIÓN

SUPONE QUE **EL INTERESADO SE PUEDE OPONER** A QUE EL RESPONSABLE REALICE UN TRATAMIENTO DE LOS DATOS PERSONALES **EN ALGUNOS SUPUESTOS**.

2. DERECHOS DE LOS CIUDADANOS EN LA PROTECCIÓN DE SUS DATOS PERSONALES

DERECHO DE SUPRESIÓN (AL OLVIDO)

SUPONE QUE EL INTERESADO PUEDA **SOLICITAR** AL RESPONSABLE LA **SUPRESIÓN DE SUS DATOS** DE CARÁCTER PERSONAL CUANDO CONCURRA ALGUNA DE LAS CIRCUNSTANCIAS PREVISTAS.

DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

SUPONE EL DERECHO DEL INTERESADO A QUE **EL RESPONSABLE DEL TRATAMIENTO LIMITE EL TRATAMIENTO** DE SUS DATOS PERSONALES.

2. DERECHOS DE LOS CIUDADANOS EN LA PROTECCIÓN DE SUS DATOS PERSONALES

DERECHO A LA PORTABILIDAD DE LOS DATOS

SUPONE QUE CUANDO EL TRATAMIENTO SE EFECTÚE POR MEDIOS AUTOMATIZADOS, EL INTERESADO RECIBA SUS **DATOS PERSONALES EN UN FORMATO ESTRUCTURADO**, DE USO COMÚN, DE LECTURA MECÁNICA E INTEROPERABLE, Y PUEDA TRANSMITIRLOS A OTRO RESPONSABLE DEL TRATAMIENTO, SIEMPRE QUE EL TRATAMIENTO SE LEGITIME EN BASE AL CONSENTIMIENTO O EN EL MARCO DE LA EJECUCIÓN DE UN CONTRATO.

CONTENIDOS

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD
2. DERECHOS DE LOS CIUDADANOS EN LA PROTECCIÓN DE SUS DATOS PERSONALES
3. **PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: MEDIDAS DE CUMPLIMIENTO EN EL RGPD**
4. LA AUDITORÍA DE PROTECCIÓN DE DATOS
5. AUDITORÍA DE SISTEMAS DE INFORMACIÓN

3. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: MEDIDAS DE CUMPLIMIENTO EN EL RGPD

EL **RESPONSABLE DEL TRATAMIENTO** O **RESPONSABLE** ES LA PERSONA FÍSICA O JURÍDICA, AUTORIDAD PÚBLICA, SERVICIO U OTRO ORGANISMO QUE, SOLO O JUNTO CON OTROS, DETERMINE LOS FINES Y MEDIOS DEL TRATAMIENTO

EL **ENCARGADO DE TRATAMIENTO** O **ENCARGADO** ES LA PERSONA FÍSICA O JURÍDICA, AUTORIDAD PÚBLICA, SERVICIO U OTRO ORGANISMO QUE TRATE DE DATOS PERSONALES POR CUENTA DEL RESPONSABLE DEL TRATAMIENTO.

LA REGULACIÓN DE LA **RELACIÓN ENTRE EL RESPONSABLE Y EL ENCARGADO DEL TRATAMIENTO** DEBE ESTABLECERSE **A TRAVÉS DE UN CONTRATO O DE UN ACTO JURÍDICO SIMILAR QUE LOS VINCULE**.

3. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: MEDIDAS DE CUMPLIMIENTO EN EL RGPD

CUANDO **DOS O MÁS RESPONSABLES** DETERMINEN CONJUNTAMENTE LOS OBJETIVOS Y LOS MEDIOS DEL TRATAMIENTO **SERÁN CONSIDERADOS CORRESPONSABLES** DEL TRATAMIENTO.

EL ENCARGADO DEL TRATAMIENTO PUEDE ESTABLECER UN RÉGIMEN DE **SUBCONTRATACIÓN**.

EL RGPD EXIGE LA **AUTORIZACIÓN PREVIA POR ESCRITO DEL RESPONSABLE** DEL TRATAMIENTO PARA QUE EL ENCARGADO DEL TRATAMIENTO PUEDA RECURRIR A OTRO ENCARGADO (*SUBENCARGADO*).

3. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: MEDIDAS DE CUMPLIMIENTO EN EL RGPD

EL **RGPD** DEFINE **REPRESENTANTE** COMO LA PERSONA FÍSICA O JURÍDICA ESTABLECIDA EN LA UNIÓN QUE, HABIENDO SIDO DESIGNADA POR ESCRITO POR EL RESPONSABLE O EL ENCARGADO DEL TRATAMIENTO, **REPRESENTE AL RESPONSABLE O AL ENCARGADO EN LO QUE RESPECTA A SUS RESPECTIVAS OBLIGACIONES EN VIRTUD DEL RGPD**.

EL **REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD),** RECOGE LA OBLIGACIÓN DE **ELABORAR UN REGISTRO DE ACTIVIDADES DE TRATAMIENTO** CONFORME A LO ESTIPULADO EN EL ARTÍCULO 30 DEL REGLAMENTO

CONTENIDOS

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD
2. DERECHOS DE LOS CIUDADANOS EN LA PROTECCIÓN DE SUS DATOS PERSONALES
3. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: MEDIDAS DE CUMPLIMIENTO EN EL RGPD
4. **LA AUDITORÍA DE PROTECCIÓN DE DATOS**
5. AUDITORÍA DE SISTEMAS DE INFORMACIÓN

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

LA PROTECCIÓN DE DATOS EN LA ORGANIZACIÓN ESTÁ ADQUIRIENDO MAYOR PROTAGONISMO DEBIDO AL **TRÁFICO DE DATOS PERSONALES Y A LAS EXIGENCIAS DE NUEVA NORMATIVA COMUNITARIA**.

POR ELLO, RESULTA **INDISPENSABLE** PROCEDER A UNA **EVALUACIÓN EN EL CUMPLIMIENTO** DE TALES DISPOSICIONES.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

UNO DE LOS **OBJETIVOS** PRINCIPALES DE LA REALIZACIÓN DE **LA AUDITORIA** EN PROTECCIÓN DE DATOS, ES **VERIFICAR LA ADAPTACIÓN DE LA ENTIDAD A LAS OBLIGACIONES** IMPUESTAS **EN LA NORMATIVA VIGENTE.**

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

ADEMÁS, SU OBJETIVO NO TIENE POR QUÉ LIMITARSE EN EXCLUSIVA, SINO QUE PODRÁ EXTENDERSE EN LO NECESARIO.

LO HABITUAL SERÁ DETERMINAR LAS POSIBLES DEBILIDADES E INCUMPLIMIENTOS, PARA **VERIFICAR EL CUMPLIMIENTO DEL PRINCIPIO DE RESPONSABILIDAD PROACTIVA**.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

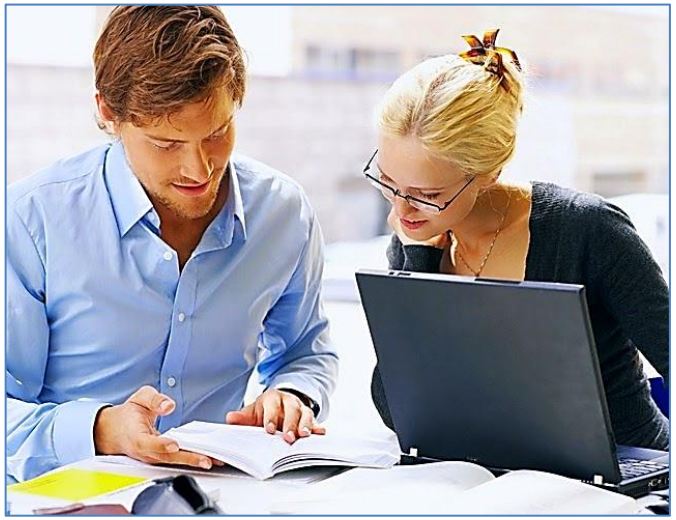
SERÁ DE VITAL IMPORTANCIA **FIJAR EL OBJETIVO DE LA AUDITORÍA** PARA ASÍ PODER DETERMINAR LAS FUENTES DE INFORMACIÓN Y DOCUMENTACIÓN, LAS PRUEBAS A PRÁCTICAS, ETC.

DE IGUAL FORMA, SABREMOS SI NECESITAREMOS **CONTAR CON UN AUDITOR O UN EQUIPO MULTIDISCIPLINAR**.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

LA AUDITORÍA DE PROTECCIÓN DE DATOS SE PUEDE LLEVAR A CABO CON UN AUDITOR INTERNO O EXTERNO.

- **AUDITOR INTERNO,** FORMA PARTE DE LA PLANTILLA DE LA EMPRESA AUDITADA, CON LA QUE MANTIENE UN CONTRATO LABORAL.
- **AUDITOR EXTERNO,** NO FORMA PARTE DE LA PLANTILLA DE LA EMPRESA AUDITADA. MANTIENE CON LA EMPRESA AUDITADA UN CONTRATO DE PRESTACIÓN DE SERVICIOS.



4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EN CUANTO **A LOS TRABAJOS REALIZADOS POR AMBOS** (ANTE UN MISMO ALCANCE) **DEBERÍAN SER SIMILARES**, YA QUE LAS TÉCNICAS UTILIZADAS EN AMBOS CASOS SON LAS MISMAS.

AMBAS **CENTRAN SU ATENCIÓN EN ASPECTOS DE CONTROL INTERNO Y EN LA EVALUACIÓN DE RIESGOS** PARA FORMULAR OBSERVACIONES QUE, JUNTO CON UNA OPINIÓN GENERAL, QUEDAN REFLEJADAS EN UN INFORME DE AUDITORÍA.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

SIN EMBARGO, SÍ QUE **EXISTEN FACTORES** QUE PUEDEN INFLUIR A LA HORA DE DECIDIR SI REALIZAR LA AUDITORÍA DE **FORMA INTERNA O EXTERNA**, COMO PUDIERAN SER:

- LA DISPONIBILIDAD DE RECURSOS INTERNOS CON EL PERFIL Y EXPERIENCIA ADECUADOS.
- ASPECTOS PRESUPUESTARIOS
- LA POSIBILIDAD DE INCLUIR EL RGPD EN LOS CICLOS DE PLANIFICACIÓN DE AUDITORÍA INTERNA
- POTENCIALES CONFLICTOS DE INTERÉS.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

SUJETOS ENCARGADOS

EN ESTE PUNTO, TENEMOS QUE **DIFERENCIAR LOS SUJETOS QUE PUEDEN PROCEDER A LA REALIZACIÓN DE AUDITORÍAS** Y QUIEN DEBE REALIZARLA:

- **SUJETOS COMPETENTES**
- **SUJETOS OBLIGADOS**

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

SUJETOS ENCARGADOS

SUJETOS COMPETENTES

NO SE EXIGIRÁ UN PERFIL CONCRETO.

EN ESTE CASO, EL SUJETO DEBERÁ **TENER PLENA INDEPENDENCIA DE LA ENTIDAD AUDITADA**, ASÍ COMO UN **PERFIL Y EXPERIENCIA APROPIADOS** PARA SU REALIZACIÓN, PUES **DEBERÁ SER CAPAZ DE VALORAR** LOS ENTORNOS Y EL GRADO DE CUMPLIMIENTO DE LA NORMATIVA Y RIESGOS, CON EL OBJETIVO DE QUE PUEDA APORTAR RECOMENDACIONES COHERENTES PARA EL TRATAMIENTO.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

SUJETOS ENCARGADOS

SUJETOS OBLIGADOS

SE **EXCLUIRÁN** A AQUELLOS SUJETOS QUE **NO REÚNAN LAS CONDICIONES NECESARIAS** PARA SU REALIZACIÓN.

"EN EL CASO DEL RGPD EL PERFIL Y EXPERIENCIA PUEDEN SER LOS DE UN EQUIPO ESPECIALIZADO Y MULTIDISCIPLINAR, Y PARECE EVIDENTE QUE UN CONOCIMIENTO ADECUADO DEL PROPIO REGLAMENTO".

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

SUJETOS ENCARGADOS

CABE DESTACAR EL PAPEL DEL **DELEGADO DE PROTECCIÓN DE DATOS**, SI LO HUBIERE, QUE SERÁ EL **RESPONSABLE DE SUPERVISAR EL CUMPLIMIENTO DE LO DISPUESTO EN EL RGPD**, DE OTRAS DISPOSICIONES DE PROTECCIÓN DE DATOS DE LA UNIÓN, DE LA **LOPDGDD 3/2018** Y DE LAS POLÍTICAS DEL RESPONSABLE O DEL ENCARGADO DEL TRATAMIENTO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES, INCLUIDA LA **ASIGNACIÓN DE RESPONSABILIDADES, LA CONCIENCIACIÓN Y FORMACIÓN DEL PERSONAL** QUE PARTICIPA EN LAS OPERACIONES DE TRATAMIENTO, Y LAS AUDITORÍAS CORRESPONDIENTES.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

¿QUÉ PRINCIPIOS MARCARÁN LA ACTIVIDAD DEL AUDITOR?

CONDUCTA ÉTICA

LOS AUDITORES SE GUIARÁN POR LO ESTABLECIDO EN LOS CÓDIGOS DE CONDUCTA.

OBJETIVIDAD

TODAS LAS CONCLUSIONES DEL PROCESO DEBERÁN REFLEJARSE EN EL INFORME DE AUDITORÍA DE FORMA VERAZ Y PRECISA.

PROFESIONALIDAD

LOS AUDITORES SERÁN PROFESIONALES EXPERTOS CON CONOCIMIENTO EN LA MATERIA, CUYOS DICTÁMENES REFLEJEN LAS EVIDENCIAS DE LA AUDITORÍA.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

¿QUÉ PRINCIPIOS MARCARÁN LA ACTIVIDAD DEL AUDITOR?

INDEPENDENCIA

LOS AUDITORES SERÁN SUJETOS OBJETIVOS E INDEPENDIENTES QUE ESTÉN LIBRES DE POSIBLES CONFLICTOS DE INTERESES.

IMPARCIALIDAD

EL AUDITOR NO PODRÁ REALIZAR AUDITORÍAS EN AQUELLAS ÁREAS EN LAS QUE ESTÉ DIRECTA O INDIRECTAMENTE INVOLUCRADO.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

AUDITORÍA DE PROTECCIÓN DE DATOS

LOS **ASPECTOS QUE DEBE EVALUAR UNA AUDITORIA** DE PROTECCIÓN DE DATOS SON LOS **PRINCIPIOS DE RESPONSABILIDAD PROACTIVA Y EL ENFOQUE AL RIESGO**.

LAS AUDITORIAS DEBERÁN DISEÑARSE Y REALIZARSE EN FUNCIÓN DEL TIPO DE ORGANIZACIÓN QUE VAYA A SER AUDITADA, ASÍ COMO DEL MOMENTO, NATURALEZA O CONTEXTO DE LOS TRATAMIENTOS QUE LA MISMA LLEVE A CABO.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

AUDITORÍA DE PROTECCIÓN DE DATOS

LA **PLANIFICACIÓN** DE CADA AUDITORÍA DEBERÁ IR PRECEDIDA DE ESE **ANÁLISIS PREVIO**. LOS **TRES GRANDES BLOQUES** DE ASPECTOS QUE DEBERÍAN EVALUARSE Y PRIORIZARSE SON:

- **ASPECTOS LEGALES**
- **ASPECTOS ORGANIZATIVOS**
- **ASPECTOS TÉCNICOS O DE SEGURIDAD**

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

AUDITORÍA DE PROTECCIÓN DE DATOS

ASPECTOS LEGALES

EL **RGPD** RECOGE UNA SERIE DE **MEDIDAS** CUYO **INCUMPLIMIENTO** PODRÍA CONLLEVAR LA **IMPOSICIÓN DE SANCIONES** Y ELLO SIN NECESIDAD DE QUE EXISTA UNA LESIÓN PREVIA DE LOS DERECHOS Y LIBERTADES DEL INTERESADO. ESTAS **MEDIDAS LEGALES** SON:

- TRATAR LOS DATOS PERSONALES CONFORME A LAS BASES LEGITIMADORAS (ARTÍCULOS 6 Y 9)
- CUMPLIR CON EL DEBER DE TRANSPARENCIA HACIA EL INTERESADO (ARTÍCULOS 12 Y 22)
- GESTIONAR LOS EJERCICIOS DE DERECHOS DE LOS INTERESADOS (ARTÍCULOS 15 A 22)

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

AUDITORÍA DE PROTECCIÓN DE DATOS

ASPECTOS LEGALES

- INCLUIR LA PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO (ARTÍCULO 25) EN CUALQUIER ACTIVIDAD QUE VAYA A SUPONER EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL
- REGULARIZAR LAS RELACIONES DE CORRESPONSABILIDAD (ARTÍCULO 26)
- REGULARIZAR LAS RELACIONES DE ENCARGO DEL TRATAMIENTO (ARTÍCULO 28)
- DISPONER DE UN REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO, (ARTÍCULO 30), EN DETERMINADOS CASOS, EL RESPONSABLE Y EL ENCARGADO DEBERÁN LLEVAR UN REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO EFECTUADAS

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

AUDITORÍA DE PROTECCIÓN DE DATOS

ASPECTOS LEGALES

- IMPLEMENTAR MEDIDAS QUE PERMITAN LA REALIZACIÓN DE UNA NOTIFICACIÓN DE UNA VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES A LA AUTORIDAD DE CONTROL Y, EN SU CASO, A LOS INTERESADOS (ARTÍCULOS 33 Y 34). DENTRO DE ESTA CATEGORÍA RESULTARÁ MUY CONVENIENTE CONTAR CON PROCEDIMIENTOS INTERNOS, NORMATIVA TAMBIÉN DE CARÁCTER INTERNO, ASÍ COMO LA REALIZACIÓN DE SIMULACROS PERIÓDICOS QUE PERMITAN REALIZAR UN CONTROL EFECTIVO
- REALIZAR UNA EVALUACIÓN DE IMPACTO (ARTÍCULO 35) Y, SI FUERA PRECISO, REALIZAR LA CONSULTA PREVIA A LA AUTORIDAD DE CONTROL (ARTÍCULO 36)
- EN CASO DE SER NECESARIO, CONTAR CON UN DELEGADO DE PROTECCIÓN DE DATOS (ARTÍCULO 37)

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

AUDITORÍA DE PROTECCIÓN DE DATOS

ASPECTOS ORGANIZATIVOS

ENTENDEMOS **RIESGO ORGANIZATIVO** A AQUEL **QUE AFECTE A LA PROPIA ESTRUCTURA DE LA ORGANIZACIÓN Y A LA TOMA DE DECISIONES** QUE GARANTICE LA REDUCCIÓN DEL RIESGO DE INCUMPLIMIENTO EN LA MATERIA.

UNOS **MECANISMOS DE GOBIERNO** QUE PERMITAN **TOMAR DECISIONES** AL NIVEL ADECUADO Y CON LA INFORMACIÓN SUFICIENTE, Y UNA **ESTRUCTURA ORGANIZATIVA** QUE PERMITA LA **INVOLUCRACIÓN Y PARTICIPACIÓN** DE TODAS LAS ÁREAS DE UNA EMPRESA EN LA PROTECCIÓN DEL DATO, DETERMINARÁN EL ÉXITO EN EL GRADO DE CUMPLIMIENTO CON **RGPD**.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

AUDITORÍA DE PROTECCIÓN DE DATOS

ASPECTOS ORGANIZATIVOS

AHORA BIEN, PARA ELLO SERÁ NECESARIO COMENZAR CON UNA CORRECTA **FORMACIÓN DE TODO EL PERSONAL**.

LA **ADOPCIÓN DE POLÍTICAS Y NORMAS INTERNAS** DIRIGIDAS A LOS EMPLEADOS, COLABORADORES Y PROVEEDORES, TANTO CON CARÁCTER GENERAL COMO FOCALIZADAS EN RELACIÓN A LAS FUNCIONES QUE DESEMPEÑEN DENTRO DE LA EMPRESA, JUGARÁ UN PAPEL DECISIVO EN ESTE OBJETIVO.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

AUDITORÍA DE PROTECCIÓN DE DATOS

ASPECTOS ORGANIZATIVOS

ALGUNOS **EJEMPLOS** DE POLÍTICAS O DE NORMAS INTERNAS PODRÍAN SER:

- POLÍTICAS CORPORATIVAS DE PROTECCIÓN DE DATOS.
- POLÍTICAS DE GOBIERNO DE LA PRIVACIDAD.
- MARCO DE CONTROLES EN MATERIA DE PROTECCIÓN DE DATOS.
- POLÍTICA SOBRE USO DE HERRAMIENTAS CORPORATIVAS, RECURSOS COMPARTIDOS, ETC.
- NORMAS INTERNAS QUE CONTENGAN LOS PRINCIPIOS Y REGLAS APLICABLES A LA CONTRATACIÓN DE PROVEEDORES.
- POLÍTICA SOBRE DISPOSITIVOS MÓVILES Y EL USO DEL TELETRABAJO.
- UN PROGRAMA DE FORMACIÓN PERIÓDICO GENERAL PARA NUEVAS INCORPORACIONES O PERSONALIZADO EN FUNCIÓN DE LAS TAREAS DESARROLLADAS DENTRO DE LA COMPAÑÍA, IMPULSARÁN LA CONCIENCIACIÓN EN ESTA MATERIA Y, POR CONSIGUIENTE, LA PROACTIVIDAD EN EL CUMPLIMIENTO DE LA NORMA.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

AUDITORÍA DE PROTECCIÓN DE DATOS

ASPECTOS TÉCNICOS O DE SEGURIDAD

EL **RGPD** SI BIEN **AVANZA MEDIDAS DE CARÁCTER TÉCNICO** QUE SE PUEDEN CONSIDERAR APROPIADAS PARA EL CUMPLIMIENTO DE LA NORMA, **NO SE PRONUNCIA** SOBRE AQUELLAS QUE GARANTIZAN LA PROTECCIÓN Y, POR CONSIGUIENTE, EL CUMPLIMIENTO DE LA NORMA.

ASÍ, LAS MEDIDAS QUE SE SEÑALAN EN EL TEXTO NORMATIVO SON **AQUELLAS QUE PERMITAN GARANTIZAR LA CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD Y RESILIENCIA** PERMANENTES DE LOS SISTEMAS Y SERVICIOS DE TRATAMIENTO EN LOS TÉRMINOS DEL ARTÍCULO 32.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

AUDITORÍA DE PROTECCIÓN DE DATOS

ASPECTOS TÉCNICOS O DE SEGURIDAD

EN CUALQUIER CASO Y DE CONFORMIDAD CON EL **PRINCIPIO DE RESPONSABILIDAD ACTIVA**, SERÁN **LAS ORGANIZACIONES** LAS QUE **DECIDAN** EN CADA MOMENTO, SEGÚN EL CONTEXTO Y LAS ACTIVIDADES DE TRATAMIENTO LLEVADAS A CABO POR LA MISMA, LA **OPORTUNIDAD Y BONDAD DE LAS MEDIDAS TÉCNICAS** A IMPLEMENTAR.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

AUDITORÍA DE PROTECCIÓN DE DATOS

ASPECTOS TÉCNICOS O DE SEGURIDAD

ALGUNOS EJEMPLOS DE MEDIDAS TÉCNICAS:

- CONTROLES TECNOLÓGICOS PARA LA SEGURIDAD DE LA INFORMACIÓN.
- MEDIDAS PARA LA CONTINUIDAD DE NEGOCIO Y RECUPERACIÓN ANTE DESASTRES.
- MEDIDAS PARA PROTEGER EL USO DE HERRAMIENTAS HABITUALES (CORREO ELECTRÓNICO) COMO ANTISPAM O ANTI PHISHING.
- PROTECCIÓN DE SITIOS WEB.
- REALIZACIÓN DE COPIAS DE SEGURIDAD Y ACTUALIZACIÓN DE SISTEMAS OPERATIVOS.
- CIFRADO DE FICHEROS Y DISCOS.
- SISTEMAS DE CONTROL DE ACCESOS.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

AUDITORÍA DE PROTECCIÓN DE DATOS

ASPECTOS TÉCNICOS O DE SEGURIDAD

- CORTAFUEGOS.
- HERRAMIENTAS QUE PERMITEN ANALIZAR Y CONTROLAR LA ACTIVIDAD DEL USUARIO EN EL ENVÍO DE INFORMACIÓN AL EXTERIOR DESDE SU PUESTO DE TRABAJO MEDIANTE LA DETECCIÓN DE FUGAS DE INFORMACIÓN.
- GESTIÓN CENTRALIZADA DE CONTRASEÑAS, CONTROL DE ACCESOS Y SESIONES: QUIÉN ACCEDE, CUÁNDO Y A QUÉ.
- GESTIÓN DE USUARIOS.
- POLÍTICAS DE RESPUESTA ANTE INCIDENCIAS Y GESTIÓN DE BRECHAS DE SEGURIDAD.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

UNA DE LAS FUNCIONES CLAVES DEL GOBIERNO CORPORATIVO EN TODOS LOS SECTORES ES **LA FUNCIÓN DE AUDITORÍA**. EL GOBIERNO DE LA PRIVACIDAD DE LOS DATOS PERSONALES FORMA PARTE DE DICHO GOBIERNO CORPORATIVO.

LAS EMPRESAS CUYOS TRATAMIENTOS DE DATOS PERSONALES ESTÁN SUJETOS A LOS REQUISITOS DEL RGPD **DEBERÍAN REALIZAR DE FORMA PERIÓDICA AUDITORÍAS DE CUMPLIMIENTO** DEL MISMO PARA EVALUAR SU NIVEL DE CUMPLIMIENTO.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

DICHAS AUDITORÍAS, PROPUESTAS NORMALMENTE DESDE LAS ÁREAS DE AUDITORÍA INTERNA DEL RESPONSABLE DE TRATAMIENTO, CONSTITUYEN **LA TERCERA LÍNEA DE DEFENSA**.

LAS **3 LÍNEAS DE DEFENSA EN CIBERSEGURIDAD SON:**

- **PRIMERA LÍNEA DE DEFENSA**: LAS PERSONAS
- **SEGUNDA LÍNEA DE DEFENSA**: LA TECNOLOGÍA Y LOS SERVICIOS
- **TERCERA LÍNEA DE DEFENSA**: LA TRANSFERENCIA DEL RIESGO

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

EL **RGPD** BRINDA UNA **MAYOR CAPACIDAD DE DISPOSICIÓN DE LOS INTERESADOS** SOBRE SUS DATOS PERSONALES Y ADEMÁS **FOMENTA LA AUTORRESPONSABILIDAD Y AUTOGESTIÓN DE LAS EMPRESAS**.

LAS AUDITORÍAS DE PROTECCIÓN DE DATOS PERSONALES DEBEN **PROPORCIONAR UNA VISIÓN INDEPENDIENTE** SOBRE EL NIVEL DE ADECUACIÓN DE LOS RESPONSABLES Y ENCARGADOS DE TRATAMIENTOS A LA LEGISLACIÓN Y NORMATIVAS RELATIVAS A LA PROTECCIÓN DE LOS DATOS PERSONALES DE LOS CIUDADANOS.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

LAS AUDITORIAS SOBRE PROTECCIÓN DE DATOS PERSONALES **DEBEN EVALUAR LOS CONTROLES DE RIESGOS SOBRE LA PROTECCIÓN DE LOS DATOS PERSONALES DEFINIDOS E IMPLEMENTADOS POR LAS EMPRESAS RELATIVOS A LA ORGANIZACIÓN, PROCESOS Y TECNOLOGÍA**.

EN LÍNEAS GENERALES, LAS ENTIDADES DEBERÍAN ESTABLECER UN PROGRAMA DE AUDITORÍA QUE TRATE UNA O MÁS NORMAS DE SISTEMAS DE GESTIÓN U OTROS REQUISITOS, REALIZADAS POR SEPARADO O EN COMBINACIÓN.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

PODEMOS CONSIDERAR **LA AUDITORÍA ES UN PROCESO QUE SE DEBE REALIZAR DE FORMA PERIÓDICA Y ENGLOBAR LAS MEDIDAS LEGALES, TÉCNICAS Y ORGANIZATIVAS DERIVADAS DE LA OBLIGACIÓN DE CUMPLIMIENTO DEL RGPD Y DE LA LOPDGDD**, ASÍ COMO DE OTRAS POLÍTICAS QUE PUDIESEN REGULAR LA ACTUACIÓN DEL RESPONSABLE O EL ENCARGADO DEL TRATAMIENTO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

EN EL DESARROLLO DE LA AUDITORÍA SE RECOMIENDA **CONSIDERAR LOS** SIGUIENTES **DOMINIOS FUNCIONALES**:

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

GOBIERNO DE LA PRIVACIDAD

CÓMO SE GOBIERNA LA PRIVACIDAD EN LA ENTIDAD, QUÉ **ROLES** ESTÁN INVOLUCRADOS, CUÁLES SON LOS **PROCEDIMIENTOS** QUE MARCA LA ORGANIZACIÓN RESPECTO A LA PROTECCIÓN DE DATOS PERSONALES. SE DEBEN EVALUAR TODAS LAS **EVIDENCIAS VINCULADAS:**

- POLÍTICA DE PRIVACIDAD.
- DEFINICIÓN DE ROLES Y FUNCIONES DE PRIVACIDAD.
- NOMBRAMIENTO Y DIFUSIÓN DE LOS RESPONSABLES DE PRIVACIDAD.
- NORMATIVA INTERNA DE PRIVACIDAD: POLÍTICAS DE PRIVACIDAD, PROCEDIMIENTOS, PROTOCOLOS, ESTÁNDARES, PROCESOS, ETC.
- IDENTIFICACIÓN DE LA AUTORIDAD DE CONTROL PRINCIPAL.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

GOBIERNO DE LA PRIVACIDAD

- ACCIONES DE COMUNICACIÓN Y PUBLICACIÓN DE LAS FUNCIONES DE PRIVACIDAD, ROLES IMPLICADOS EN LA ORGANIZACIÓN, ASÍ COMO POLÍTICAS Y PROCEDIMIENTOS VINCULADOS A LA PROTECCIÓN DE DATOS PERSONALES.
- REVISIÓN DE COMUNICACIONES A LA AUTORIDAD DE CONTROL. POR EJEMPLO, INSCRIPCIÓN DEL DPD.
- REVISIÓN DE INSPECCIONES, SANCIONES, CONSULTAS A LA AUTORIDAD DE CONTROL, ETC.
- CÓDIGOS DE CONDUCTAS Y/O CERTIFICACIONES.
- NORMAS CORPORATIVAS VINCULANTES.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

DELEGADOS DE PROTECCIÓN DE DATOS

LA FORMALIZACIÓN DE LA FIGURA Y LAS FUNCIONES DEL **DPD**:

- ANÁLISIS DE LA NECESIDAD DEL DPD Y DECISIÓN TOMADA POR LA ENTIDAD.
- ACTA DE NOMBRAMIENTO DEL DPD SI APLICA.
- ORGANIGRAMA DE ENTIDAD, POSICIÓN DEL DPD/DPO Y NIVEL DE REPORTE.
- CANALES DE COMUNICACIÓN INTERNOS Y EXTERNOS CON EL DPD.
- NOMBRAMIENTO Y DIFUSIÓN DE LOS RESPONSABLES DE PRIVACIDAD.
- ANÁLISIS DE COMPATIBILIDAD/INCOMPATIBILIDAD DE FUNCIONES.
- ANÁLISIS DE LA CUALIFICACIÓN Y DIMENSIONAMIENTO DE LA OFICINA DEL EL DPD.
- REVISIÓN DE FUNCIONES.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

LICITUD Y TRANSPARENCIA

SE DEBE EVALUAR SI TODOS LOS TRATAMIENTOS SON LÍCITOS Y LA IDONEIDAD DE LA BASE LEGITIMADORA UTILIZADA.

- LICITUD DE LOS TRATAMIENTOS (ART.6)
- TRANSPARENCIA EN LA INFORMACIÓN FACILITADA DE LOS TRATAMIENTOS (ART.12-13-14)
- ARGUMENTACIÓN/ANÁLISIS DE LOS TRATAMIENTOS BASADOS EN INTERÉS LEGÍTIMO
- REVISIÓN DE CONSENTIMIENTOS
- REVISIÓN DE CONTRATOS
- REVISIÓN DE CLÁUSULAS INFORMATIVAS
- FOOTERS DE PRIVACIDAD EN CORREOS ELECTRÓNICOS
- POLÍTICA DE PRIVACIDAD EN LAS WEBS
- POLÍTICAS DE PRIVACIDAD EN ZONAS DE ACCESO
- CONSULTA A SISTEMAS DE EXCLUSIÓN PUBLICITARIA

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

GESTIÓN DE DERECHOS DE LOS INTERESADOS

CÓMO SE ACTÚA ANTE EL EJERCICIO DE DERECHOS; CUÁL ES EL PROCEDIMIENTO A SEGUIR, QUIÉN INTERVIENE; QUIÉN DEBE CONTESTAR, CONTESTACIÓN EN TIEMPO Y FORMA.

- PROCEDIMIENTO DE GESTIÓN DE DERECHOS.
- SISTEMAS DE INFORMACIÓN DE LOS DERECHOS DE LOS USUARIOS.
- FORMULARIOS DE SOLICITUD.
- CANALES DE COMUNICACIÓN.
- ROLES QUE INTERVIENEN.
- LISTADO DE EJERCICIOS DE DERECHO EJERCITADOS Y REVISIÓN DE EJECUCIÓN DE PROCEDIMIENTO Y RESPUESTAS.
- REVISIÓN DE SU EFECTIVA APLICACIÓN TANTO EN BASES DE DATOS ESTRUCTURADAS COMO NO ESTRUCTURADAS.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

SE DEBE EVALUAR CÓMO SE HA ORQUESTADO EL ANÁLISIS DE LA PRIVACIDAD DESDE EL DISEÑO.

- PROCEDIMIENTO DE PRIVACY BY DESIGN Y PRIVACY BY DEFAULT
- PRINCIPIOS DE MINIMIZACIÓN DE DATOS.
- POLÍTICA DE CONSERVACIÓN DE DATOS.
- LISTADO DE INICIATIVAS Y EVALUACIÓN DE PRIVACIDAD DESDE EL DISEÑO: EVIDENCIAS DE SU SEGUIMIENTO (ACTAS DE REUNIONES CON LA PARTICIPACIÓN DEL DPD, REQUERIMIENTOS, SEGUIMIENTO, RESOLUCIÓN DE CONSULTAS...).
- EVALUAR SI EXISTEN REQUERIMIENTOS PARA PODER EJERCER EL BLOQUEO Y LIMITACIÓN DE TRATAMIENTO DE DATOS PERSONALES DESDE EL DISEÑO.
- REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

- REVISIÓN DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO, COMPLETITUD DEL MISMO, ADECUADA Y ACTUALIZADA LA DESCRIPCIÓN DE LOS MISMOS.
- REVISIÓN DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO, COMPLETITUD DEL MISMO, ADECUADA Y ACTUALIZADA DESCRIPCIÓN DE LOS MISMOS.
- CUESTIONARIOS DE VALIDACIÓN DE LAS DISTINTAS ÁREAS.
- FINALIDAD DE LOS TRATAMIENTOS.
- PROGRAMAS DE GESTIÓN UTILIZADOS.
- REVISIÓN DE PLAZOS DE CONSERVACIÓN DE LA INFORMACIÓN CON RESPECTO A LA POLÍTICA DE CONSERVACIÓN.
- REVISIÓN DE ACCESIBILIDAD DE LOS DATOS SEGÚN CORRESPONDA AL TRATAMIENTO EN EL CICLO DEL DATO.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

ANÁLISIS DE RIESGO Y EVALUACIÓN DE IMPACTO

REVISIÓN DEL MODELO DE RIESGOS DE PRIVACIDAD A DISTINTOS NIVELES Y DE LA OPERATIVA LLEVADA A CABO EN ESTE SENTIDO.

- METODOLOGÍA DE ANÁLISIS DE RIESGOS DE DATOS PERSONALES.
- PROCEDIMIENTOS DE EVALUACIÓN DE IMPACTO EN DATOS PERSONALES (ART.35).
- MODELO/FORMALIZACIÓN DE LOS PIA'S.
- REALIZACIÓN DE ANÁLISIS DE RIESGOS DE DATOS PERSONALES DE LA ENTIDAD.
- REVISIÓN DE LOS PROCESOS DE EVALUACIÓN OBJETIVA - ANÁLISIS DE RIESGOS DE DATOS PERSONALES
- REVISIÓN DE LAS EVALUACIONES DE IMPACTOS EN DATOS PERSONALES EXISTENTES.
- REVISIÓN DE CONSULTAS A AUTORIDADES DE CONTROL.
- VALORACIÓN DE LAS MEDIDAS LEGALES, ORGANIZATIVAS Y TÉCNICAS APLICADAS PARA REDUCIR LOS RIESGOS INHERENTES A LOS TRATAMIENTOS.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

MEDIDAS DE SEGURIDAD

LA REVISIÓN DE LAS MEDIDAS DE SEGURIDAD VINCULADAS A LOS TRATAMIENTOS DE DATOS PERSONALES **CONTEMPLA TODO SU CICLO**: LA PARTE DE ESTABLECIMIENTO DE LAS MISMAS EN EL **MOMENTO INICIAL DE DISEÑO** DE LA INICIATIVA (PRIVACY BY DESIGN) Y LAS QUE DERIVAN DEL **ANÁLISIS DE RIESGOS** Y, EN SU CASO, LA APLICACIÓN DE LAS MISMAS EN **LOS TRATAMIENTOS** QUE DEBEN RECOGERSE EN EL REGISTRO DE ACTIVIDADES DEL TRATAMIENTO (ARTÍCULO 30 DEL RGPD) **Y REVISAR SU CORRECTO FUNCIONAMIENTO**, ASÍ COMO ACTUALIZACIÓN EN CASO NECESARIO.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

MEDIDAS DE SEGURIDAD

- RELACIÓN DE MEDIDAS TÉCNICAS Y ORGANIZATIVAS VINCULADAS A LOS ANÁLISIS DE RIESGO
- EVALUAR SU ADECUADA IMPLANTACIÓN
- LAS MEDIDAS PUEDEN SER DE DISTINTO TIPO Y NATURALEZA. SE RECOMIENDA VER LA RELACIÓN DE MEDIDAS VINCULADAS A RIESGO QUE SE EJEMPLIFICA EN EL ANEXO VI: CATÁLOGO DE AMENAZAS Y POSIBLES SOLUCIONES DE LA GUÍA PRÁCTICA PARA LAS EVALUACIONES DE IMPACTO EN LA PROTECCIÓN DE LOS DATOS SUJETAS AL RGPD DE LA AEPD
- ALGUNAS DE LAS MEDIDAS TÉCNICAS MÁS FRECUENTES IMPLANTADAS PARA INCREMENTAR LA INTEGRIDAD, DISPONIBILIDAD, CONFIDENCIALIDAD Y RESILIENCIA DE LA INFORMACIÓN PERSONAL SON:
  - SISTEMAS DE AUTENTICACIÓN DE SEGUROS BASADOS, EN DOBLE FACTOR: TOKEN DE UN SOLO USO, BIOMÉTRICOS, ETC.
  - CIFRADO DE LA INFORMACIÓN
  - PSEUDOANONIMIZACIÓN QUE DIFICULTE LA IDENTIFICACIÓN DE LOS INTERESADOS
  - SISTEMAS DE ALTA DISPONIBILIDAD

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

RESPONSABILIDAD Y FORMACIÓN

RESPONSABLE DEL CUMPLIMIENTO Y DEBERÁ SER CAPAZ DE DEMOSTRARLO.

- MANTENIMIENTO DE LOS REGISTROS NECESARIOS (DERECHOS INTERESADOS, INCIDENCIAS, ACCESOS, ETC.)
- CONTROLES PERIÓDICOS DE CUMPLIMIENTO EN MATERIA DE PROTECCIÓN DE DATOS
- PLAN DE FORMACIÓN Y CONCIENCIACIÓN EN MATERIA DE PROTECCIÓN DE DATOS
- EVALUACIÓN DE COMPLETITUD, IDONEIDAD DE CONTENIDOS DE PROTECCIÓN DATOS
- SE PODRÍA VALORAR ENTRE LAS INICIATIVAS DE FORMACIÓN DESARROLLADAS: EL TIPO DE FORMACIÓN REALIZADA (GENERAL, POR DEPARTAMENTOS, ETC.): PERIODICIDAD DE LA MISMA (SEMESTRAL, ANUAL): AUDIENCIAS CONTEMPLADAS (IDENTIFICACIÓN FIGURAS CRÍTICAS, ET, RT); ÁMBITO TERRITORIAL (CENTRALIZADA, DISTRIBUIDA, FORMACIÓN DE FORMADORES)
- ACREDITACIÓN DE LA FORMACIÓN REALIZADA Y DE LA ASISTENCIA A LA MISMA
- VALORACIÓN DE INDICADORES

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

ENCARGADOS DEL TRATAMIENTO

PERSONA FÍSICA O JURÍDICA, AUTORIDAD PÚBLICA, SERVICIO U OTRO ORGANISMO QUE TRATE DATOS PERSONALES POR CUENTA DEL RESPONSABLE DE TRATAMIENTO.

- PROCEDIMIENTO DE VERIFICACIÓN DEL CUMPLIMIENTO POR LOS ENCARGADOS DE TRATAMIENTO DE SUS OBLIGACIONES
- ANÁLISIS DE IDONEIDAD ENCARGADOS DE TRATAMIENTO
- CUESTIONARIO/EVALUACIÓN DE PRIVACIDAD.
- PLANIFICACIÓN DE REVISIONES DE ENCARGADOS DE TRATAMIENTO.
- MODELOS DE CONTRATO DE ENCARGOS DE TRATAMIENTO CON ACCESO A DATOS PERSONALES.
- ADHESIONES A CERTIFICACIONES O CÓDIGOS DE CONDUCTAS.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

CORRESPONSABILIDAD (ARTÍCULO 26)

LOS ESCENARIOS DE CORRESPONSABILIDAD SE DETALLAN EN EL **RGPD** Y SE ESTÁ INCREMENTANDO EL NÚMERO DE TRATAMIENTOS EN LOS QUE SE ADOPTA ESTA RELACIÓN ENTRE RESPONSABLES QUE DETERMINAN CONJUNTAMENTE LOS OBJETIVOS Y LOS MEDIOS DEL TRATAMIENTO.

- REVISIÓN DE LOS ACUERDOS DE CORRESPONSABILIDAD DE TRATAMIENTOS.
- REVISIÓN PUNTO DE CONTACTO DE LOS INTERESADOS DEL TRATAMIENTO.
- REVISIÓN DE COORDINACIÓN ENTRE LOS CORRESPONSABLES PARA CUMPLIMIENTO DE OBLIGACIONES FRENTE A LOS INTERESADOS.
- REVISIÓN DE CÓMO SE ABORDA EL DEBER DE INFORMACIÓN (ART. 13 Y 14 DEL RGPD).

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

CORRESPONSABILIDAD (ARTÍCULO 26)

SI ADEMÁS DE LOS TRATAMIENTOS REALIZADOS EN EL ROL DE RESPONSABLE DEL TRATAMIENTO, LA ENTIDAD AUDITADA PRETENDE INCORPORAR EN EL ALCANCE DE LA AUDITORÍA LOS TRATAMIENTOS DE DATOS QUE REALIZA EN CALIDAD DE ENCARGADO DEL TRATAMIENTO, HABRÁN DE CONTEMPLARSE LOS SIGUIENTES DOMINIOS FUNCIONALES:

- **REGISTRO DE ACTIVIDADES**
- **SUBENCARGADOS DEL TRATAMIENTO**
- **NOTIFICACIONES DE BRECHAS DE SEGURIDAD**
- **MEDIDAS DE SEGURIDAD**
- **TRANSFERENCIAS INTERNACIONALES**
- **OBLIGACIONES CONTRACTUALES**

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

CORRESPONSABILIDAD (ARTÍCULO 26)

NOTIFICACIONES DE BRECHAS DE SEGURIDAD

LA REVISIÓN DEL MODELO ESTABLECIDO PARA ACTUAR ANTE BRECHAS DE SEGURIDAD Y EFECTIVIDAD OPERATIVA DEL MISMO, EN PARTICULAR, LA OBLIGACIÓN DE NOTIFICAR LAS BRECHAS AL RESPONSABLE DEL TRATAMIENTO.

MEDIDAS DE SEGURIDAD:

LA REVISIÓN DE LAS MEDIDAS DE SEGURIDAD VINCULADAS A LOS TRATAMIENTOS DE DATOS PERSONALES SEGÚN LAS INSTRUCCIONES DEL RESPONSABLE DEL TRATAMIENTO Y LAS IMPLEMENTADAS POR DEFECTO POR EL ENCARGADO.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

CORRESPONSABILIDAD (ARTÍCULO 26)

TRANSFERENCIAS INTERNACIONALES

LA REVISIÓN DE LA REGULARIZACIÓN DE TRANSFERENCIAS INTERNACIONALES A LOS SUBENCARGADOS UBICADAS EN PAÍSES FUERA DEL ESPACIO ECONÓMICO EUROPEO.

OBLIGACIONES CONTRACTUALES

LA REVISIÓN DE CUMPLIMIENTO DE LAS OBLIGACIONES ESTABLECIDAS EN EL ARTÍCULO 28 DEL RGPD.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

EL PROCESO DE AUDITORÍA

CORRESPONSABILIDAD (ARTÍCULO 26)

REGISTRO DE ACTIVIDADES

LA REVISIÓN DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO QUE SE REALIZAN POR CUENTA DE LOS RESPONSABLES DE TRATAMIENTO.

SUBENCARGADOS DEL TRATAMIENTO

LA REVISIÓN DE LAS MEDIDAS IMPLEMENTADAS PARA GARANTIZAR QUE LOS SUBENCARGADOS OTORGAN GARANTÍAS SUFICIENTES RESPECTO AL TRATAMIENTO DE DATOS QUE REALIZAN, ASÍ COMO LA FIRMA DE LOS ACUERDOS CON DICHOS TERCEROS.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

ELABORACIÓN DEL INFORME DE AUDITORÍA

CONFORME A LO ESTABLECIDO EN LA NORMA **ISO 19001** DE AUDITORÍAS DE SISTEMAS DE GESTIÓN, PODEMOS DISTINGUIR LAS SIGUIENTES **FASES** FUNDAMENTALES **EN EL PROCESO DE AUDITORÍA**:

1. **INICIO DE LA AUDITORÍA**
2. **PREPARACIÓN DE LAS ACTIVIDADES DE LA AUDITORÍA**
3. **REALIZACIÓN DE LA AUDITORÍA**
4. **INFORME: PREPARACIÓN Y DISTRIBUCIÓN DEL INFORME DE AUDITORÍA**
5. **FINALIZACIÓN DE LA AUDITORÍA**
6. **SEGUIMIENTO: REALIZACIÓN DE ACTIVIDADES DE SEGUIMIENTO**

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

ELABORACIÓN DEL INFORME DE AUDITORÍA

NOS VAMOS A CENTRAR EN LA FASE 4 *INFORME: PREPARACIÓN Y DISTRIBUCIÓN DEL INFORME DE AUDITORÍA.*

LA AUDITORÍA DEBE PRODUCIR UNOS RESULTADOS Y UNAS CONCLUSIONES QUE SE PLASMAN EN UN INFORME.

PODEMOS DIFERENCIAR LAS SIGUIENTES FASES:

1. **PREPARACIÓN DEL INFORME**
2. **DISTRIBUCIÓN DEL INFORME DE AUDITORIA**

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

ELABORACIÓN DEL INFORME DE AUDITORÍA

1. PREPARACIÓN DEL INFORME

- REALIZAR UNA COMUNICACIÓN CLARA DE LOS ASPECTOS MÁS RELEVANTES IDENTIFICADOS EN LA AUDITORÍA. EN EL INFORME DE AUDITORÍA PODRÁN REFLEJARSE EN UN APARTADO INDEPENDIENTE.
- INCLUIR TODAS LAS CONFORMIDADES Y NO CONFORMIDADES.
- RELACIONAR DE FORMA CLARA Y CONCRETA LAS RECOMENDACIONES DERIVADAS DEL ANÁLISIS REALIZADO, JUSTIFICANDO LAS MISMAS, ASOCIÁNDOLAS A LAS NO CONFORMIDADES.
- EL INFORME DE AUDITORÍA DEBE COMPONERSE DE UN INFORME EJECUTIVO Y UN INFORME DETALLADO, QUE RECOJA EN DETALLE EL TRABAJO REALIZADO Y LAS CONCLUSIONES.
- EL GRADO DE CUMPLIMIENTO DE LOS CRITERIOS DE LA AUDITORÍA.
- LAS OPINIONES DIVERGENTES QUE, EN SU CASO, PUEDAN HABER SURGIDO.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

ELABORACIÓN DEL INFORME DE AUDITORÍA

2. DISTRIBUCIÓN DEL INFORME DE AUDITORIA

- EL INFORME DEBERÁ EMITIRSE DENTRO DEL TIEMPO ACORDADO, MOTIVÁNDOSE LOS RETRASOS EN CASO DE EXISTIR.
- EL BORRADOR DEL INFORME DEBERÁ FACILITARSE AL RESPONSABLE O ENCARGADO DEL TRATAMIENTO PARA SU REVISIÓN.
- DEBERÁ DISTRIBUIRSE ENTRE LAS PARTES INTERESADAS PERTINENTES DEFINIDAS EN EL PLAN DE AUDITORÍA, GARANTIZÁNDOSE EN TODO CASO LA CONFIDENCIALIDAD DE SU CONTENIDO.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

ELABORACIÓN DEL INFORME DE AUDITORÍA

2. DISTRIBUCIÓN DEL INFORME DE AUDITORIA

- LAS RECOMENDACIONES DEL AUDITOR DEBEN FACILITARSE PARA SU ANÁLISIS AL RESPONSABLE O ENCARGADO DEL TRATAMIENTO. EL RESULTADO DE CADA RECOMENDACIÓN PODRÁ SER EL SIGUIENTE:
  - PODRÁ ACEPTARSE, EN CUYO CASO EL RESPONSABLE O ENCARGADO DEL TRATAMIENTO TENDRÍA QUE INDICAR CÓMO Y CUÁNDO SE LLEVARÍA A CABO LA RECOMENDACIÓN.
  - PODRÁ ACEPTARSE CON AJUSTES, INDICANDO CÓMO Y CUÁNDO SE LLEVARÍA A CABO LA RECOMENDACIÓN AJUSTADA, EN CUYO CASO EL AUDITOR TENDRÍA QUE VALORAR LOS AJUSTES PROPUESTOS Y DICTAMINAR SI ACEPTA O NO EL AJUSTE.
  - PODRÁ RECHAZARSE, EN CUYO CASO EL RESPONSABLE O ENCARGADO DEL TRATAMIENTO TENDRÍA QUE INDICAR LOS MOTIVOS POR LOS QUE SE RECHAZA. EL AUDITOR TENDRÍA QUE VALORAR LAS CAUSAS DEL RECHACE, Y DICTAMINAR SI LO ACEPTA O NO.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

ELABORACIÓN DEL INFORME DE AUDITORÍA

EL INFORME DE AUDITORÍA ES UNA HERRAMIENTA QUE PERMITE:

- **REALIZAR UNA CORRECTA VALORACIÓN DEL RIESGO** DE LOS PROCESOS Y PROCEDIMIENTOS Y SU ALINEAMIENTO CON LA NORMATIVA APLICABLE
- **INFORMAR DEL NIVEL DE CUMPLIMIENTO NORMATIVO** A LA ALTA DIRECCIÓN DE LA ENTIDAD.

DEBERÁ SER **UN FIEL REFLEJO DEL PROCESO DE AUDITORÍA QUE SE HA REALIZADO,** DESCRIBIENDO FIELMENTE LAS LABORES Y ACCIONES REALIZADAS, LAS EVIDENCIAS QUE RESPALDAN DICHOS HALLAZGOS Y LOS RESULTADOS Y CONCLUSIONES DE DICHO PROCESO.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

FINALIZACIÓN DE LA AUDITORIA

LA AUDITORÍA SE ENTENDERÁ FINALIZADA CUANDO SE HAN LLEVADO A CABO TODAS LAS ACTIVIDADES DE AUDITORÍA PLANIFICADAS.

A SU FINALIZACIÓN, DEBERÁ CONSERVARSE TODA LA DOCUMENTACIÓN RELATIVA A LA AUDITORÍA DE ACUERDO CON LO ESTABLECIDO EN EL PROGRAMA DE AUDITORÍA.

EN EL SUPUESTO DE EXISTIR NECESIDAD POR PARTE DE LOS AUDITORES DE DIVULGACIÓN DEL CONTENIDO DEL INFORME, DEBERÁN SER INFORMADOS, LO ANTES POSIBLE, EL RESPONSABLE Y EL ENCARGADO DEL TRATAMIENTO

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

FINALIZACIÓN DE LA AUDITORIA

DURANTE LA **PRESENTACIÓN DE RESULTADOS DE LA AUDITORIA** SE REALIZARÁ UNA **EXPOSICIÓN ANALÍTICA Y DEPURADA** DE LOS PRINCIPALES **HALLAZGOS, OBSERVACIONES Y CONCLUSIONES** RECOGIDOS EN EL **INFORME FINAL**, DESTACANDO LOS ASPECTOS MÁS RELEVANTES DEL TRABAJO REALIZADO.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

FINALIZACIÓN DE LA AUDITORIA

RESULTA OPORTUNO **PRESENTAR LOS RESULTADOS DE LA AUDITORÍA** CON SUFICIENTE PRECISIÓN Y CLARIDAD, **SIGUIENDO UN ORDEN O ESTRUCTURA** CONGRUENTE CON EL INFORME FINAL, YA QUE, EN CIERTA MEDIDA, LA EFICACIA DE LOS OBJETIVOS PERSEGUIDOS CON LA AUDITORÍA, ASÍ COMO LA EJECUCIÓN DE LAS ACCIONES Y COMPROMISOS DERIVADAS DE LA MISMA, DEPENDERÁN DEL DISCERNIMIENTO DE TALES RESULTADOS Y CONCLUSIONES.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

FINALIZACIÓN DE LA AUDITORIA

LOS RESULTADOS DE LA AUDITORÍA SE COMUNICARÁN A LOS CORRESPONDIENTES PERFILES PROFESIONALES.

EN UNA PRIMERA FASE, ES RECOMENDABLE QUE LOS RESULTADOS SE COMUNIQUEN AL DELEGADO DE PROTECCIÓN DE DATOS O AL ÁREA DE CUMPLIMIENTO EN CASO DE QUE NO SE HAYA NOMBRADO UN DPO.

EN CASO DE REALIZARSE LA AUDITORÍA POR UNA ENTIDAD EXTERNA, LOS RESULTADOS ASIMISMO SE DEBERÍAN COMUNICAR AL DEPARTAMENTO DE AUDITORÍA INTERNA.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

FINALIZACIÓN DE LA AUDITORIA

EN UNA FASE POSTERIOR, LOS RESULTADOS SE DEBERÍAN COMUNICAR A LA ALTA DIRECCIÓN DE LA ENTIDAD, DE NUEVO, EN FUNCIÓN DEL MARCO ORGANIZATIVO DE LA ENTIDAD Y LOS PROTOCOLOS DE GESTIÓN DE CUMPLIMIENTO IMPLEMENTADOS.

EN CASO DE UNA AUDITORÍA EXTERNA, PREVIO ACUERDO CON EL ÁREA INTERNA DEL RESPONSABLE DEL TRATAMIENTO QUE HAYA IMPULSADO SU REALIZACIÓN, LA COMUNICACIÓN A LA ALTA DIRECCIÓN PUEDE REALIZARSE POR LA PROPIA ENTIDAD EXTERNA.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

FINALIZACIÓN DE LA AUDITORIA

UNA VEZ PRESENTADOS LOS RESULTADOS, CONVENDRÍA **OBTENER UNA CONFIRMACIÓN POR PARTE DE LOS INTERLOCUTORES DE LA ENTIDAD AUDITADA** QUE ASISTIERON A LA REUNIÓN DE CIERRE, A PARTIR DE LA CUAL SE MANIFIESTE QUE LOS RESULTADOS DE LA AUDITORÍA HAN SIDO CONOCIDOS, COMPRENDIDOS, CONTRASTADOS Y ACEPTADOS.

DICHA CONFIRMACIÓN PODRÁ DOCUMENTARSE MEDIANTE LA EMISIÓN DE UN "**ACTA DE LA REUNIÓN DE CIERRE Y PRESENTACIÓN DE RESULTADOS DE AUDITORÍA**", O DOCUMENTO SIMILAR SUSCRITO POR LOS PARTICIPANTES DE DICHA REUNIÓN.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

REALIZACIÓN DE ACTIVIDADES DE SEGUIMIENTO

RESULTA HABITUAL QUE COMO CONSECUENCIA DE LA PRESENTACIÓN DE RESULTADOS DE LA AUDITORIA SE **DERIVEN COMPROMISOS Y/O TAREAS A SER REALIZADAS**, POSTERIORMENTE, POR PARTE DE LA ENTIDAD AUDITADA **CON EL FIN DE SUBSANAR LAS NO CONFORMIDADES** RESIDUALES QUE HAYAN PERSISTIDO TRAS EL CIERRE DE LA AUDITORÍA.

TALES COMPROMISOS Y ACCIONES CORRECTIVAS SURGEN DE LAS RECOMENDACIONES O ACCIONES CORRECTIVAS QUE EL EQUIPO AUDITOR HA SEÑALADO EN SU INFORME FINAL.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

REALIZACIÓN DE ACTIVIDADES DE SEGUIMIENTO

POR LO TANTO, SE PROCURARÁ ACORDAR LA MANERA EN QUE LA ORGANIZACIÓN ATENDERÁ DICHAS RECOMENDACIONES O PROPUESTAS DE MEJOR CUMPLIMIENTO, ESTIMANDO: LA FECHA DE EJECUCIÓN, QUIÉN SERÁ EL RESPONSABLE DE LLEVARLAS A CABO Y QUIEN SERÁ EL RESPONSABLE DE VERIFICAR SU SEGUIMIENTO, EJECUCIÓN O CIERRE DE LAS ACTIVIDADES PENDIENTES Y CUANDO SE REALIZARÁ DICHA VERIFICACIÓN.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

REALIZACIÓN DE ACTIVIDADES DE SEGUIMIENTO

LA DESIGNACIÓN DE ESTAS TAREAS PODRÁ REALIZARSE SIGUIENDO LA METODOLOGÍA **RACI** (RESPONSIBLE, ACCOUNTABLE, CONSULTED, INFORMED), UTILIZADA PARA LA COORDINACIÓN O GESTIÓN DE PROYECTOS A PARTIR DE LOS CUALES SE ATRIBUYEN RESPONSABILIDADES A LOS DIFERENTES ACTORES QUE PARTICIPAN EN LA EJECUCIÓN DE LAS ACTIVIDADES QUE, EN ESTE CASO, SERÍAN LAS QUE HAYAN QUEDADO PENDIENTES DE SUBSANACIÓN TRAS EL CIERRE DE LA AUDITORIA.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

REALIZACIÓN DE ACTIVIDADES DE SEGUIMIENTO

EL SEGUIMIENTO O EJECUCIÓN DE ESTAS ACTIVIDADES RESIDUALES DEBERÁ ALINEARSE CON LOS RESULTADOS DE LA AUDITORÍA, EN EL SENTIDO EN QUE PARA PODER CERRAR CADA UNA DE LAS TAREAS PENDIENTES SE HABRÁ DE CONFIRMAR QUE SE HAYAN EFECTUADO SATISFACTORIAMENTE LAS ACCIONES CORRECTIVAS O RECOMENDACIONES PARA SUBSANAR LAS NO CONFORMIDADES DETECTADAS.

ASIMISMO, PARA EL SEGUIMIENTO DE CADA TAREA/RESPONSABILIDAD ASIGNADA, PODRÁN ACORDARSE:

- FECHA DE COMPROMISO DE EJECUCIÓN DE LA ACCIÓN CORRECTIVA;
- FECHA DE SEGUIMIENTO O COMPROBACIÓN DE LA EJECUCIÓN DE DICHA TAREA.

4. LA AUDITORÍA DE PROTECCIÓN DE DATOS

RESUMEN

LA AUDITORÍA DEBE PRODUCIR UNOS **RESULTADOS Y UNAS CONCLUSIONES** QUE SE PLASMAN EN **UN INFORME**.

DURANTE LA PRESENTACIÓN DE RESULTADOS DE LA AUDITORIA SE REALIZARÁ UNA EXPOSICIÓN ANALÍTICA Y DEPURADA DE LOS PRINCIPALES HALLAZGOS, OBSERVACIONES Y CONCLUSIONES RECOGIDOS EN EL INFORME FINAL.

CONTENIDOS

1. LEGITIMACIÓN PARA EL TRATAMIENTO DE LOS DATOS PERSONALES EN EL RGPD
2. DERECHOS DE LOS CIUDADANOS EN LA PROTECCIÓN DE SUS DATOS PERSONALES
3. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: MEDIDAS DE CUMPLIMIENTO EN EL RGPD
4. LA AUDITORÍA DE PROTECCIÓN DE DATOS
5. **AUDITORÍA DE SISTEMAS DE INFORMACIÓN**

5. AUDITORÍA DE SISTEMAS DE INFORMACIÓN

LAS **TECNOLOGÍAS DE LA INFORMACIÓN**, EN PARTICULAR INTERNET Y LA TELEFONÍA MÓVIL, CONSTITUYEN LO QUE HOY SE CONSIDERA LA SOCIEDAD DE LA INFORMACIÓN.

LA **SEGURIDAD DE LA INFORMACIÓN** TIENE COMO OBJETIVO LA PROTECCIÓN DE SISTEMAS E INFORMACIÓN EN CUANTO A QUE ÉSTOS SIEMPRE SE ENCUENTREN ACCESIBLES, QUE NO SUFRAN ALTERACIONES MALINTENCIONADAS O POR ERROR Y QUE SU ACCESO SE PERMITA EXCLUSIVAMENTE A PERSONAS AUTORIZADAS EN LA FORMA DEBIDA.

5. AUDITORÍA DE SISTEMAS DE INFORMACIÓN

LA INFORMACIÓN Y LOS PROCESOS, SISTEMAS Y REDES DE APOYO SON ACTIVOS COMERCIALES MUY IMPORTANTES. DEFINIR, LOGRAR, MANTENER Y MEJORAR LA SEGURIDAD DE LA INFORMACIÓN SON FACTORES ESENCIALES PARA MANTENER UNA VENTAJA COMPETITIVA, EL FLUJO DE CAJA, RENTABILIDAD, OBSERVANCIA LEGAL E IMAGEN COMERCIAL.

EL **PRINCIPAL OBJETIVO** QUE PERSIGUE LA SEGURIDAD DE LA INFORMACIÓN ES PROTEGER LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN Y LOS DATOS, CON INDEPENDENCIA DE LA FORMA EN QUE ÉSTOS SE PUEDAN OBTENER.

5. AUDITORÍA DE SISTEMAS DE INFORMACIÓN

LA **FAMILIA DE NORMAS ISO/IEC 27000** ES UN CONJUNTO DE ESTÁNDARES, EN FASE DE DESARROLLO LA MAYORÍA, QUE PROPORCIONAN UN MARCO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN UTILIZABLE POR CUALQUIER TIPO DE ORGANIZACIÓN, PÚBLICA O PRIVADA, CON INDEPENDENCIA DEL TAMAÑO DE LA MISMA.

LA **ISO/IEC 27002** VA ORIENTADA A LA SEGURIDAD DE LA INFORMACIÓN EN LAS EMPRESAS U ORGANIZACIONES, DE MODO QUE LAS PROBABILIDADES DE SER AFECTADOS POR ROBO, DAÑO O PÉRDIDA DE INFORMACIÓN SE MINIMICEN AL MÁXIMO.

5. AUDITORÍA DE SISTEMAS DE INFORMACIÓN

EL **RESPONSABLE DEL FICHERO** DEBE TENER EN CUENTA QUE RECOGER, TRATAR Y CEDER DATOS DE CARÁCTER PERSONAL VULNERANDO LOS PRINCIPIOS Y GARANTÍAS ESTABLECIDAS EN LA LOPD 3/2018 PUEDE SER CONSTITUTIVO DE INFRACCIÓN LEVE, GRAVE O MUY GRAVE SEGÚN SEA EL CASO DE QUE SE TRATE.

ESTO ES TODO