IFCT0109. SEGURIDAD INFORMÁTICA

MF0490_3 GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

UD01

GESTIÓN DE LA SEGURIDAD Y NORMATIVAS

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. INTRODUCCIÓN
2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN
4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
5. NORMATIVAS MÁS FRECUENTEMENTE UTILIZADAS PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA

1. INTRODUCCIÓN

EN LA ACTUALIDAD LAS TECNOLOGÍAS DE LA INFORMACIÓN TIENEN **UN PAPEL MUY IMPORTANTE** EN CUALQUIER ORGANIZACIÓN, INTEGRÁNDOSE PLENAMENTE EN LOS DISTINTOS PROCEDIMIENTOS DE GESTIÓN DE LAS MISMAS.

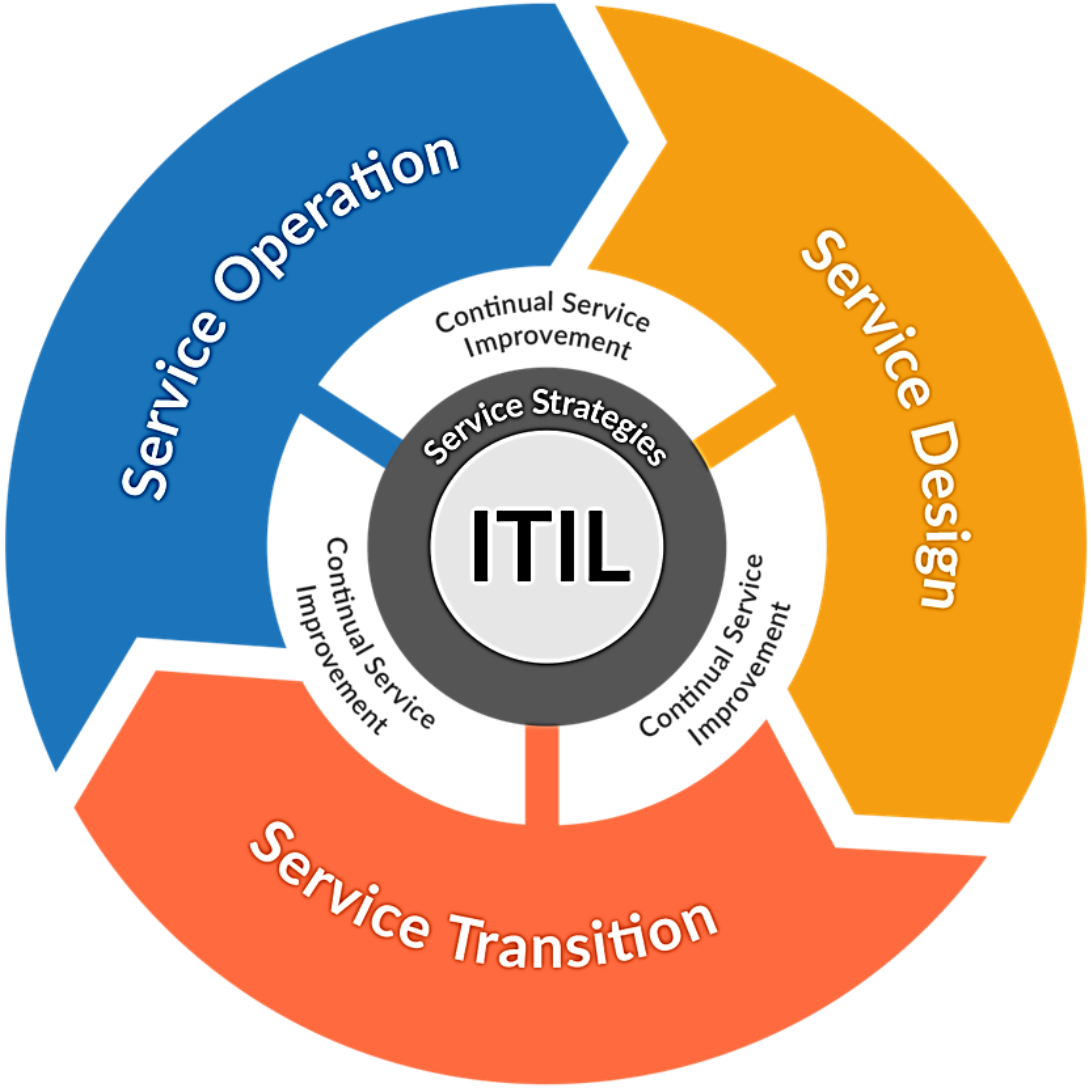
ES **IMPRESCINDIBLE** TENER UN *CONOCIMIENTO BÁSICO Y GENÉRICO SOBRE LAS DISTINTAS NORMATIVAS* REFERENTES A LAS TECNOLOGÍAS DE LA INFORMACIÓN.

1. INTRODUCCIÓN

SE PROCEDERÁ A OFRECER UNA VISIÓN GENERAL DEL **CÓDIGO DE BUENAS PRÁCTICAS PARA EFECTUAR UNA ADECUADA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**, LLAMADO TAMBIÉN **NORMA ISO/IEC 27002**

1. INTRODUCCIÓN

A CONTINUACIÓN, SE ESTUDIARÁ LA **LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN (METODOLOGÍA ITIL)** HERRAMIENTA FUNDAMENTAL **CON UNA SERIE DE RECOMENDACIONES** PARA QUE LA **INTEGRACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN CON LOS SERVICIOS DE LA ORGANIZACIÓN** SE REALICE CORRECTAMENTE



1. INTRODUCCIÓN

LAS TECNOLOGÍAS DE LA INFORMACIÓN VAN ESTRECHAMENTE LIGADAS AL **TRATAMIENTO DE DATOS PERSONALES**, YA QUE MUY FRECUENTEMENTE LOS DATOS PERSONALES FORMAN PARTE DE LA BASE DE DATOS DE CUALQUIER ORGANIZACIÓN.

SE DA UNA ESPECIAL IMPORTANCIA A LA NORMATIVA REFERENTE AL TRATAMIENTO DE DATOS PERSONALES, PARA EVITAR INCURRIR EN CUALQUIER INFRACCIÓN DEBIDO AL DESCONOCIMIENTO DE LAS NORMAS FUNDAMENTALES.

1. INTRODUCCIÓN

ADEMÁS DE UNA CORRECTA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN AUTOMATIZADA, TAMBIÉN ES VITAL MANTENER UN NIVEL ADECUADO DE **SEGURIDAD FÍSICA** PARA EVITAR LA INTROMISIÓN DE PERSONAS NO AUTORIZADAS O PARA PREVENIR UN MAL USO DE LOS FICHEROS MANUALES QUE CONTENGAN INFORMACIÓN DELICADA.

TERMINAREMOS CON UNA SERIE DE **MEDIDAS Y RECOMENDACIONES** QUE APORTEN A LA ORGANIZACIÓN UN NIVEL DE SEGURIDAD FÍSICA ÓPTIMO.

CONTENIDOS

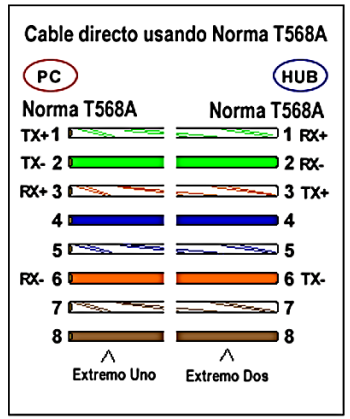
1. INTRODUCCIÓN
2. **NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**
3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN
4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
5. NORMATIVAS MÁS FRECUENTEMENTE UTILIZADAS PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA

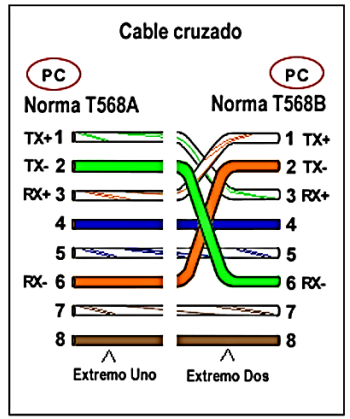
2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

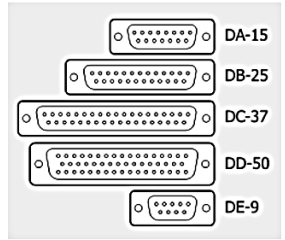
MOTIVACIÓN PARA EL USO DE NORMAS

LAS NORMAS INTERNACIONALES SALVAN LAS BARRERAS TÉCNICAS DE LAS DIFERENTES NORMAS DE CADA NACIÓN.

LA ADOPCIÓN DE NORMAS INTERNACIONALES **PERMITE CREAR NORMAS NACIONALES EQUIVALENTES** CON DIFERENCIAS EN SU APARIENCIA, USO DE SÍMBOLOS, UNIDADES DE MEDIDAS Y POSIBLES CONFLICTOS CON LA NORMATIVA GUBERNAMENTAL O REQUISITOS ESPECÍFICOS DEL SECTOR DE QUE SE TRATE.







2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

AGENTES QUE INTERVIENEN EN LA NORMALIZACIÓN Y CERTIFICACIÓN

LAS NORMAS O ESTÁNDARES INTERNACIONALES SON EL PRODUCTO DE DIFERENTES ORGANIZACIONES. LOS AGENTES QUE INTERVIENEN EN EL PROCESO DE NORMALIZACIÓN Y CERTIFICACIÓN SON:

- **ORGANIZACIONES DE NORMALIZACIÓN**
- **ORGANIZACIONES DE ACREDITACIÓN**
- **ENTIDADES DE CERTIFICACIÓN**
- **CONSULTORES**
- **AUDITORES**

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

AGENTES QUE INTERVIENEN EN LA NORMALIZACIÓN Y CERTIFICACIÓN

ORGANIZACIONES DE NORMALIZACIÓN

LOS ORGANISMOS O AGENCIAS NACIONALES E INTERNACIONALES **TIENEN LA TAREA DE FIJAR NORMAS TÉCNICAS QUE ESTABLEZCAN LA TERMINOLOGÍA**, **LA CLASIFICACIÓN, LAS DIRECTRICES, LAS ESPECIFICACIONES, LOS ATRIBUTOS, LAS CARACTERÍSTICAS, LOS MÉTODOS DE PRUEBA** O **LAS PRESCRIPCIONES** APLICABLES A UN **PRODUCTO, PROCESO O SERVICIO** CON EL FIN DE PRESERVAR LA SEGURIDAD, LA PROTECCIÓN AL CONSUMIDOR, AL MEDIO AMBIENTE, A LA SALUD DE LAS PERSONAS Y ANIMALES, Y FAVORECER EL EFECTIVO INTERCAMBIO DE BIENES.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

AGENTES QUE INTERVIENEN EN LA NORMALIZACIÓN Y CERTIFICACIÓN

ORGANIZACIONES DE NORMALIZACIÓN

INTERNACIONALES:

- ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN **(ISO)**
- COMISIÓN ELECTROTÉCNICA INTERNACIONAL **(IEC)**
- UNIÓN INTERNACIONAL DE TELECOMUNICACIONES **(ITU)**

EUROPEAS :

- COMITÉ EUROPEO DE NORMALIZACIÓN **(CEN)**
- COMITÉ EUROPEO DE NORMALIZACIÓN ELECTROTÉCNICA **(CENELEC)**
- INSTITUTO EUROPEO DE NORMAS DE TELECOMUNICACIONES **(ETSI)**

ESPAÑOLAS:

- ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN **(AENOR)**

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

AGENTES QUE INTERVIENEN EN LA NORMALIZACIÓN Y CERTIFICACIÓN

ORGANIZACIONES DE ACREDITACIÓN

SU FUNCIÓN ES **EVALUAR**, MEDIANTE AUDITORÍAS, **QUE LOS ORGANISMOS EVALUADORES** DE LA CONFORMIDAD (LABORATORIOS, ENTIDADES DE INSPECCIÓN, DE CERTIFICACIÓN Y DE VERIFICACIÓN O VALIDACIÓN, ENTRE OTROS) **SEAN TÉCNICAMENTE COMPETENTES**.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

AGENTES QUE INTERVIENEN EN LA NORMALIZACIÓN Y CERTIFICACIÓN

ORGANIZACIONES DE ACREDITACIÓN

INTERNACIONALES:

- FORO INTERNACIONAL DE ACREDITACIÓN **(IAF)**
- RED INTERNACIONAL DE CERTIFICACIÓN **(IQNET)**

EUROPEAS :

- EUROPEAN CO-OPERATION FOR ACCREDITATION **(EA)**

ESPAÑOLAS:

- ENTIDAD NACIONAL DE ACREDITACIÓN **(ENAC)**

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

AGENTES QUE INTERVIENEN EN LA NORMALIZACIÓN Y CERTIFICACIÓN

ENTIDADES DE CERTIFICACIÓN

LAS ENTIDADES CERTIFICADORAS **EMITEN CERTIFICADOS** QUE GARANTIZAN (MEDIANTE AUDITORÍAS) LA IMPLANTACIÓN CORRECTA DE LAS NORMAS.

EN ESPAÑA:

- ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN (AENOR)
- BUREAU VERITAS IBERIA, S.L.
- IVAC-INSTITUTO DE CERTIFICACIÓN, S.L.
- LGAI TECHNOLOGICAL CENTER, S.A.
- OCA INSTITUTO DE CERTIFICACIÓN, S.L. (UNIPERSONAL)

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

AGENTES QUE INTERVIENEN EN LA NORMALIZACIÓN Y CERTIFICACIÓN

CONSULTORES

SON PROFESIONALES O EMPRESAS QUE **ASESORAN A EMPRESAS Y ORGANIZACIONES** EN:

- OBTENER LA CERTIFICACIÓN CORRESPONDIENTE
- PROCESO DE IMPLANTACIÓN
- FORMACIÓN INTERNA DE LOS TRABAJADORES

DEBEN CONTAR CON FORMACIÓN ESPECÍFICA AVALADA POR UN EXAMEN.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

AGENTES QUE INTERVIENEN EN LA NORMALIZACIÓN Y CERTIFICACIÓN

AUDITORES

SON **PROFESIONALES** QUE CUENTAN **CON LA ACREDITACIÓN QUE PERMITE REALIZAR LA AUDITORÍA** QUE GARANTICE LA CORRECTA IMPLANTACIÓN DE LA NORMA.

PARA ALCANZAR ESTE TÍTULO, **DEBE CONTAR CON UNA FORMACIÓN ESPECÍFICA Y SUPERAR UN EXAMEN** A LOS EFECTOS.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

LA NORMA **ISO/IEC 27002** SE CREA BAJO LA COORDINACIÓN DE LA INTERNATIONAL **ORGANIZATION FOR STANDARATION** (**ISO**) Y LA **COMISIÓN ELECTROTÉCNICA INTERNACIONAL** (**IEC**). INICIALMENTE, ERA NORMATIVA **ISO 17799.**

SE ENGLOBA DENTRO DE UN CONJUNTO DE NORMATIVAS **ISO/IEC 2700X** QUE REGULAN TEMAS DE SEGURIDAD EN LOS ÁMBITOS DIGITAL Y ELECTRÓNICO.

IEC

ISO International Organization for Standardization

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ISO 27000

VOCABULARIO QUE SE VA A UTILIZAR EN LAS NORMAS INCLUIDAS EN TODA LA SERIE.

ISO/IEC 27001

SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS.

ISO/IEC 27002

GUÍA DE BUENAS PRÁCTICAS QUE DESCRIBE LOS DISTINTOS OBJETIVOS DE CONTROL Y CONTROLES RECOMENDADOS PARA MANTENER UN NIVEL DE SEGURIDAD DE LA INFORMACIÓN ÓPTIMO.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

ISO/IEC 27002 ESTÁ FORMADA POR LAS SECCIONES:

1. INTRODUCCIÓN
2. CAMPO DE APLICACIÓN
3. TÉRMINOS Y DEFINICIONES
4. ESTRUCTURA DEL ESTÁNDAR
5. EVALUACIÓN Y TRATAMIENTO DEL RIESGO.
6. POLÍTICA DE SEGURIDAD
7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
8. GESTIÓN DE ACTIVOS
9. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS
10. SEGURIDAD FÍSICA Y DEL ENTORNO
11. GESTIÓN DE COMUNICACIONES Y OPERACIONES
12. CONTROL DE ACCESOS
13. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN
14. GESTIÓN DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN
15. GESTIÓN DE CONTINUIDAD DEL NEGOCIO
16. CUMPLIMIENTOS LEGALES.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

1. INTRODUCCIÓN

LA INFORMACIÓN ES UN ACTIVO ESPECIALMENTE VALIOSO EN CUALQUIER ORGANIZACIÓN, SOBRE TODO SI SE TIENE EN CUENTA QUE EL **ENTORNO EMPRESARIAL ESTÁ CADA VEZ MÁS INTERCONECTADO** DEBIDO AL FENÓMENO DE LA GLOBALIZACIÓN.

ESTE FENÓMENO PROVOCA QUE **LA INFORMACIÓN CADA VEZ SEA MÁS VULNERABLE ANTE ATAQUES Y AMENAZAS**, POR LO QUE RESULTA **IMPRESCINDIBLE QUE ESTÉ PROTEGIDA** CON UN NIVEL DE SEGURIDAD LO MÁS ELEVADO POSIBLE.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

1. INTRODUCCIÓN

PARA ESTABLECER SISTEMAS DE INFORMACIÓN SEGUROS, **LA NORMA ISO 27002 ESTABLECE UNA SERIE DE PASOS IMPORTANTES** QUE DEBE REALIZAR CADA EMPRESA U ORGANIZACIÓN:

- **IDENTIFICAR LOS REQUERIMIENTOS DE SEGURIDAD**, EVALUANDO LOS DISTINTOS RIESGOS DE LA ORGANIZACIÓN
- **EVALUAR METÓDICAMENTE LOS RIESGOS DE SEGURIDAD** PARA ESTABLECER PRIORIDADES DE GESTIÓN DE RIESGOS Y CONTROLES
- **SELECCIÓN DE LOS CONTROLES ADECUADOS** QUE SE DEBEN IMPLANTAR PARA REDUCIR LOS RIESGOS A UN NIVEL ACEPTABLE
- **ESTABLECIMIENTO DE UN PUNTO DE INICIO DE LA SEGURIDAD** COMO, POR EJEMPLO, IMPLANTAR UNA SERIE DE CONTROLES COMO ESENCIALES
- **IDENTIFICACIÓN DE LOS FACTORES CRÍTICOS** DE ÉXITO EN LA IMPLEMENTACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA ORGANIZACIÓN
- **DESARROLLO Y ADAPTACIÓN DE CONTROLES PROPIOS**

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

2. OBJETO Y CAMPO DE APLICACIÓN

LOS **OBJETIVOS DE CONTROL Y LOS CONTROLES** DE LA **ISO 27002** SE DISEÑAN PARA QUE *SE* ***SATISFAGAN LOS REQUERIMIENTOS IDENTIFICADOS MEDIANTE LA EVALUACIÓN DE LOS RIESGOS DE LA ORGANIZACIÓN***.

ESTA NORMATIVA TAMBIÉN **SIRVE COMO ORIENTACIÓN DE PARTIDA PARA LAS ORGANIZACIONES CON EL FIN DE ELABORAR E IMPLANTAR SUS PROPIAS MEDIDAS DE SEGURIDAD Y PARA FOMENTAR UN AMBIENTE DE CONFIANZA Y PARTICIPACIÓN** DE LAS DISTINTAS ÁREAS ORGANIZATIVAS EN LAS ACTIVIDADES RELACIONADAS CON LA SEGURIDAD DE LA INFORMACIÓN

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

3. TÉRMINOS Y DEFINICIONES

SE RECOGEN LAS DEFINICIONES DE LOS TÉRMINOS MÁS UTILIZADOS EN ESTA NORMATIVA:

- **SEGURIDAD DE LA INFORMACIÓN:** *PRESERVACIÓN DE LA CONFIDENCIALIDAD, INTEGRACIÓN Y DISPONIBILIDAD DE LA INFORMACIÓN*. TAMBIÉN PUEDE INVOLUCRAR OTRAS PROPIEDADES COMO LA AUTENTICIDAD, RESPONSABILIDAD, NO REPUDIACIÓN Y CONFIABILIDAD.
- **INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN**: *EVENTO O SERIE DE EVENTOS INESPERADOS DE SEGURIDAD DE LA INFORMACIÓN QUE TIENEN UNA PROBABILIDAD SIGNIFICATIVA DE COMPROMETER LAS OPERACIONES COMERCIALES Y AMENAZAR LA SEGURIDAD DE LA INFORMACIÓN.*

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

3. TÉRMINOS Y DEFINICIONES

- **ANÁLISIS DEL RIESGO:** *USO SISTEMÁTICO DE LA INFORMACIÓN PARA IDENTIFICAR LAS FUENTES Y CALCULAR EL RIESGO.*
- **EVALUACIÓN DEL RIESGO:** *PROCESO DE COMPARAR EL RIESGO ESTIMADO CON UN CRITERIO DE RIESGO DADO PARA DETERMINAR LA IMPORTANCIA DEL RIESGO.*
- **GESTIÓN DEL RIESGO:** *ACTIVIDADES PARA DIRIGIR Y CONTROLAR UNA ORGANIZACIÓN CON RELACIÓN AL RIESGO.*
- **TRATAMIENTO DEL RIESGO:** *PROCESO DE SELECCIÓN E IMPLEMENTACIÓN DE MEDIDAS PARA MODIFICAR EL RIESGO.*
- **CONTROL:** *MEDIOS PARA MANEJAR EL RIESGO, INCLUYENDO POLÍTICAS, PROCEDIMIENTOS, PRÁCTICAS O ESTRUCTURAS ORGANIZACIONALES, QUE PUEDEN SER ADMINISTRATIVAS, TÉCNICAS, DE GESTIÓN O DE NATURALEZA LEGAL.*

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

4. ESTRUCTURA DE ESTA NORMA

LA NORMA **ISO/IEC 27002** CONTIENE **14 CAPÍTULOS** QUE INCLUYEN **35 OBJETIVOS DE CONTROL** Y **114 CONTROLES,** ADEMÁS DE UNA CLÁUSULA DE INTRODUCCIÓN QUE TRATA LA EVALUACIÓN Y EL TRATAMIENTO DEL RIESGO.

CADA **CAPÍTULO,** QUE DEFINE OBJETIVOS DE CONTROL, CONTIENE UNO O MÁS **CONTROLES**. EL ORDEN DE LOS CAPÍTULOS DE ESTA NORMA NO IMPLICA UN ORDEN DE IMPORTANCIA.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

4. ESTRUCTURA DE ESTA NORMA

CADA CATEGORÍA PRINCIPAL DE CONTROLES DE SEGURIDAD CONTIENE:

A. **UN OBJETIVO DEL CONTROL** QUE ESTABLECE QUÉ ES LO QUE SE QUIERE CONSEGUIR;

B. **UNO O MÁS CONTROLES** QUE PUEDEN SER APLICADOS **PARA CONSEGUIR EL OBJETIVO DEL CONTROL.**

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

4. ESTRUCTURA DE ESTA NORMA

LAS DESCRIPCIONES DE CADA CONTROL SE ESTRUCTURAN DE LA SIGUIENTE MANERA:

- **CONTROL**
- **GUÍA DE IMPLANTACIÓN**
- **INFORMACIÓN ADICIONAL**

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

4. ESTRUCTURA DE ESTA NORMA

CONTROL

DEFINE LA DECLARACIÓN DEL CONTROL ESPECÍFICO PARA CONSEGUIR EL OBJETIVO DEL CONTROL.

GUÍA DE IMPLANTACIÓN

PROPORCIONA INFORMACIÓN MÁS DETALLADA PARA DAR APOYO A LA IMPLANTACIÓN DEL CONTROL Y LA CONSECUCIÓN DEL OBJETIVO DEL CONTROL. ALGUNAS DE ESTAS DIRECTRICES PUEDEN NO SER APROPIADAS O SUFICIENTES PARA TODOS LOS CASOS, PUDIENDO NO ADECUARSE A LOS REQUISITOS DE CONTROL ESPECÍFICOS PARA LA ORGANIZACIÓN.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

4. ESTRUCTURA DE ESTA NORMA

INFORMACIÓN ADICIONAL

PROPORCIONA INFORMACIÓN ADICIONAL, CUYA CONSIDERACIÓN PUEDE SER NECESARIA, POR EJEMPLO, CONSIDERACIONES LEGALES Y REFERENCIAS A OTRAS NORMAS. SI NO EXISTE INFORMACIÓN ADICIONAL ESTE APARTADO NO SE INCLUYE.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

4. ESTRUCTURA DE ESTA NORMA

CAPÍTULOS DE CONTROLES DE SEGURIDAD

- 5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
- 6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
- 7. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS
- 8. GESTIÓN DE ACTIVOS
- 9. CONTROL DE ACCESO
- 10. CRIPTOGRAFÍA
- 11. SEGURIDAD FÍSICA Y DEL ENTORNO
- 12. SEGURIDAD DE LAS OPERACIONES
- 13. SEGURIDAD DEL AS COMUNICACIONES
- 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN
- 15. RELACIÓN CON PROVEEDORES
- 16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
- 17. ASPECTOS DE SEGURIDAD DE INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
- 18. CUMPLIMIENTO

5. **POLÍTICAS DE SEGURIDAD.**
   - 5.1 Directrices de la Dirección en seguridad de la información.
     - 5.1.1 Conjunto de políticas para la seguridad de la información.
     - 5.1.2 Revisión de las políticas para la seguridad de la información.
6. **ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.**
   - 6.1 Organización interna.
     - 6.1.1 Asignación de responsabilidades para la segur. de la información.
     - 6.1.2 Segregación de tareas.
     - 6.1.3 Contacto con las autoridades.
     - 6.1.4 Contacto con grupos de interés especial.
     - 6.1.5 Seguridad de la información en la gestión de proyectos.
   - 6.2 Dispositivos para movilidad y teletrabajo.
     - 6.2.1 Política de uso de dispositivos para movilidad.
     - 6.2.2 Teletrabajo.
7. **SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**
   - 7.1 Antes de la contratación.
     - 7.1.1 Investigación de antecedentes.
     - 7.1.2 Términos y condiciones de contratación.
   - 7.2 Durante la contratación.
     - 7.2.1 Responsabilidades de gestión.
     - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
     - 7.2.3 Proceso disciplinario.
   - 7.3 Cese o cambio de puesto de trabajo.
     - 7.3.1 Cese o cambio de puesto de trabajo.
8. **GESTIÓN DE ACTIVOS.**
   - 8.1 Responsabilidad sobre los activos.
     - 8.1.1 Inventario de activos.
     - 8.1.2 Propiedad de los activos.
     - 8.1.3 Uso aceptable de los activos.
     - 8.1.4 Devolución de activos.
   - 8.2 Clasificación de la información.
     - 8.2.1 Directrices de clasificación.
     - 8.2.2 Etiquetado y manipulado de la información.
     - 8.2.3 Manipulación de activos.
   - 8.3 Manejo de los soportes de almacenamiento.
     - 8.3.1 Gestión de soportes extraíbles.
     - 8.3.2 Eliminación de soportes.
     - 8.3.3 Soportes físicos en tránsito.
9. **CONTROL DE ACCESOS.**
   - 9.1 Requisitos de negocio para el control de accesos.
     - 9.1.1 Política de control de accesos.
     - 9.1.2 Control de acceso a las redes y servicios asociados.
   - 9.2 Gestión de acceso de usuario.
     - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
     - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
     - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
     - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
     - 9.2.5 Revisión de los derechos de acceso de los usuarios.
     - 9.2.6 Retirada o adaptación de los derechos de acceso
   - 9.3 Responsabilidades del usuario.
     - 9.3.1 Uso de información confidencial para la autenticación.
   - 9.4 Control de acceso a sistemas y aplicaciones.
     - 9.4.1 Restricción del acceso a la información.
     - 9.4.2 Procedimientos seguros de inicio de sesión.
     - 9.4.3 Gestión de contraseñas de usuario.
     - 9.4.4 Uso de herramientas de administración de sistemas.
     - 9.4.5 Control de acceso al código fuente de los programas.
10. **CIFRADO.**
    - 10.1 Controles criptográficos.
      - 10.1.1 Política de uso de los controles criptográficos.
      - 10.1.2 Gestión de claves.
11. **SEGURIDAD FÍSICA Y AMBIENTAL.**
    - 11.1 Áreas seguras.
      - 11.1.1 Perímetro de seguridad física.
      - 11.1.2 Controles físicos de entrada.
      - 11.1.3 Seguridad de oficinas, despachos y recursos.
      - 11.1.4 Protección contra las amenazas externas y ambientales.
      - 11.1.5 El trabajo en áreas seguras.
      - 11.1.6 Áreas de acceso público, carga y descarga.
    - 11.2 Seguridad de los equipos.
      - 11.2.1 Emplazamiento y protección de equipos.
      - 11.2.2 Instalaciones de suministro.
      - 11.2.3 Seguridad del cableado.
      - 11.2.4 Mantenimiento de los equipos.
      - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
      - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
      - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
      - 11.2.8 Equipo informático de usuario desatendido.
      - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. **SEGURIDAD EN LA OPERATIVA.**
    - 12.1 Responsabilidades y procedimientos de operación.
      - 12.1.1 Documentación de procedimientos de operación.
      - 12.1.2 Gestión de cambios.
      - 12.1.3 Gestión de capacidades.
      - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
    - 12.2 Protección contra código malicioso.
      - 12.2.1 Controles contra el código malicioso.
    - 12.3 Copias de seguridad.
      - 12.3.1 Copias de seguridad de la información.
    - 12.4 Registro de actividad y supervisión.
      - 12.4.1 Registro y gestión de eventos de actividad.
      - 12.4.2 Protección de los registros de información.
      - 12.4.3 Registros de actividad del administrador y operador del sistema.
      - 12.4.4 Sincronización de relojes.
    - 12.5 Control del software en explotación.
      - 12.5.1 Instalación del software en sistemas en producción.
    - 12.6 Gestión de la vulnerabilidad técnica.
      - 12.6.1 Gestión de las vulnerabilidades técnicas.
      - 12.6.2 Restricciones en la instalación de software.
    - 12.7 Consideraciones de las auditorías de los sistemas de información.
      - 12.7.1 Controles de auditoría de los sistemas de información.
13. **SEGURIDAD EN LAS TELECOMUNICACIONES.**
    - 13.1 Gestión de la seguridad en las redes.
      - 13.1.1 Controles de red.
      - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
      - 13.1.3 Segregación de redes.
    - 13.2 Intercambio de información con partes externas.
      - 13.2.1 Políticas y procedimientos de intercambio de información.
      - 13.2.2 Acuerdos de intercambio.
      - 13.2.3 Mensajería electrónica.
      - 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

14. **ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**
    - 14.1 Requisitos de seguridad de los sistemas de información.
      - 14.1.1 Análisis y especificación de los requisitos de seguridad.
      - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
      - 14.1.3 Protección de las transacciones por redes telemáticas.
    - 14.2 Seguridad en los procesos de desarrollo y soporte.
      - 14.2.1 Política de desarrollo seguro de software.
      - 14.2.2 Procedimientos de control de cambios en los sistemas.
      - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
      - 14.2.4 Restricciones a los cambios en los paquetes de software.
      - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
      - 14.2.6 Seguridad en entornos de desarrollo.
      - 14.2.7 Externalización del desarrollo de software.
      - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
      - 14.2.9 Pruebas de aceptación.
    - 14.3 Datos de prueba.
      - 14.3.1 Protección de los datos utilizados en pruebas.
15. **RELACIONES CON SUMINISTRADORES.**
    - 15.1 Seguridad de la información en las relaciones con suministradores.
      - 15.1.1 Política de seguridad de la información para suministradores.
      - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
      - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
    - 15.2 Gestión de la prestación del servicio por suministradores.
      - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
      - 15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. **GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**
    - 16.1 Gestión de incidentes de seguridad de la información y mejoras.
      - 16.1.1 Responsabilidades y procedimientos.
      - 16.1.2 Notificación de los eventos de seguridad de la información.
      - 16.1.3 Notificación de puntos débiles de la seguridad.
      - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
      - 16.1.5 Respuesta a los incidentes de seguridad.
      - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
      - 16.1.7 Recopilación de evidencias.
17. **ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**
    - 17.1 Continuidad de la seguridad de la información.
      - 17.1.1 Planificación de la continuidad de la seguridad de la información.
      - 17.1.2 Implantación de la continuidad de la seguridad de la información.
      - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
    - 17.2 Redundancias.
      - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
18. **CUMPLIMIENTO.**
    - 18.1 Cumplimiento de los requisitos legales y contractuales.
      - 18.1.1 Identificación de la legislación aplicable.
      - 18.1.2 Derechos de propiedad intelectual (DPI).
      - 18.1.3 Protección de los registros de la organización.
      - 18.1.4 Protección de datos y privacidad de la información personal.
      - 18.1.5 Regulación de los controles criptográficos.
    - 18.2 Revisiones de la seguridad de la información.
      - 18.2.1 Revisión independiente de la seguridad de la información.
      - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
      - 18.2.3 Comprobación del cumplimiento.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

LA DIRECCIÓN APRUEBA UN DOCUMENTO DONDE SE RECOGE UNA **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN** ACORDE CON SUS OBJETIVOS PRINCIPALES. ESTE DOCUMENTO ESTÁ A DISPOSICIÓN DE TODOS LOS EMPLEADOS Y DE AQUELLOS AGENTES EXTERNOS RELEVANTES PARA LA ORGANIZACIÓN.

SE REALIZA UNA **REVISIÓN PERIÓDICA Y SISTEMÁTICA** DEL DOCUMENTO Y DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

CADA CATEGORÍA DE SEGURIDAD CONTIENE UN OBJETIVO DE CONTROL Y UNO O MÁS CONTROLES QUE SE PUEDEN APLICAR PARA LOGRAR DICHO OBJETIVO.

REALIZARLA TAMBIÉN CUANDO OCURRAN CAMBIOS RELEVANTES QUE PUEDAN NECESITAR UNA MODIFICACIÓN DE POLÍTICA.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

CATEGORÍAS	CONTROLES
5.1 DIRECTRICES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN
	5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

ES NECESARIO ESTABLECER UNA ESTRUCTURA ORGANIZATIVA QUE COMPROMETA A TODOS LOS **AGENTES INTERNOS** Y **AGENTES EXTERNOS**.

EN CUANTO A ORGANIZACIÓN INTERNA, ES NECESARIO EL ESTABLECIMIENTO DE UNA ESTRUCTURA FIRME DE RECURSOS TÉCNICOS CAPACES DE IMPLANTAR Y MANTENER UN SISTEMA SEGURO DE GESTIÓN DE INFORMACIÓN.

A NIVEL EXTERNO, SE DEBE ASEGURAR QUE EL ACCESO DE AGENTES EXTERNOS A LA INFORMACIÓN NO IMPLIQUE UNA REDUCCIÓN DE LA SEGURIDAD DE LA MISMA.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

CATEGORÍAS	CONTROLES
6.1 ORGANIZACIÓN INTERNA	6.1.1 ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN
	6.1.2 SEGREGACIÓN DE TAREAS
	6.1.3 CONTACTO CON LAS AUTORIDADES
	6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL
	6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS
6.2 LOS DISPOSITIVOS MÓVILES Y EL TELETRABAJO	6.2.1 POLÍTICA DE DISPOSITIVOS MÓVILES
	6.2.2 TELETRABAJO

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

7. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS

SE ESTABLECEN UNA SERIE DE **CONTROLES QUE PREVENGAN UN USO INADECUADO DE LA INFORMACIÓN** POR PARTE DE LOS EMPLEADOS **ANTES** DE TRABAJAR EN LA EMPRESA, **DURANTE** SU PERÍODO DE TRABAJO Y UNA VEZ SE HA **EXTINGUIDO** SU CONTRATO DE TRABAJO CON LA MISMA.

SE ESTABLECEN UNA SERIE DE OBLIGACIONES CONTRACTUALES QUE COMPROMETAN A TODOS LOS EMPLEADOS, CONTRATISTAS, PROVEEDORES Y DEMÁS USUARIOS A CUMPLIR CON UNOS COMPROMISOS, FUNCIONES Y RESPONSABILIDADES.

TAMBIÉN SE ESTABLECE LA DEFINICIÓN Y DOCUMENTACIÓN ESPECÍFICA DE CADA UNO DE **LOS ROLES** DE LOS EMPLEADOS Y USUARIOS DE LA INFORMACIÓN, EN CONCORDANCIA CON LA POLÍTICA DE SEGURIDAD DE LA ORGANIZACIÓN.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

7. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS

CATEGORÍAS	CONTROLES
7.1 ANTES DEL EMPLEO	7.1.1 INVESTIGACIÓN DE ANTECEDENTES
	7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO
7.2 DURANTE EL EMPLEO	7.2.1 RESPONSABILIDADES DE GESTIÓN
	7.2.2 CONCIENCIACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN
	7.2.3 PROCESO DISCIPLINARIO
7.3 FINALIZACIÓN DEL EMPLEO O CAMBIO EN EL PUESTO DE TRABAJO	7.3.1 RESPONSABILIDADES ANTE LA FINALIZACIÓN O CAMBIO

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

8. GESTIÓN DE ACTIVOS

LA ORGANIZACIÓN REALIZA UN INVENTARIO DE TODOS SUS ACTIVOS (**LA INFORMACIÓN ES CONSIDERADA COMO UN ACTIVO INTANGIBLE DE LA ORGANIZACIÓN**).

LOS ACTIVOS DEBEN ESTAR CORRECTAMENTE IDENTIFICADOS EN UN DOCUMENTO ELABORADO PARA ELLO **Y**, ADEMÁS, **DEBEN SER IDENTIFICADOS LOS PROPIETARIOS** DE CADA UNO DE ELLOS (CUYA RESPONSABILIDAD SOBRE LOS ARCHIVOS TAMBIÉN DEBE QUEDAR REFLEJADA EN ESTA DOCUMENTACIÓN).

LA INFORMACIÓN HAY QUE CLASIFICARLA SEGÚN EL GRADO DE CONFIDENCIALIDAD E IMPORTANCIA QUE TENGA, PERMITIENDO ASIGNAR UN NIVEL DE PROTECCIÓN ADICIONAL A AQUELLA INFORMACIÓN CUYA IMPORTANCIA O CONFIDENCIALIDAD SEA MAYOR.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

8. GESTIÓN DE ACTIVOS

CATEGORÍAS	CONTROLES
8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS	8.1.1 INVENTARIO DE ACTIVOS
	8.1.2 PROPIEDAD DE LOS ACTIVOS
	8.1.3 USO ACEPTABLE DE LOS ACTIVOS
	8.1.4 DEVOLUCIÓN DE ACTIVOS
8.2 CLASIFICACIÓN DE LA INFORMACIÓN	8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN
	8.2.2 ETIQUETADO DE LA INFORMACIÓN
	8.2.3 MANIPULADO DE LA INFORMACIÓN
8.3 MANIPULACIÓN DE LOS SOPORTES	8.3.1 GESTIÓN DE SOPORTES EXTRAÍBLES
	8.3.2 ELIMINACIÓN DE SOPORTES
	8.3.3 SOPORTES FÍSICOS EN TRÁNSITO

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

9. CONTROL DE ACCESO

LA ORGANIZACIÓN DEBE ESTABLECER UNA SERIE DE PROCEDIMIENTOS FORMALES QUE SIRVAN **PARA ASEGURAR EL ACCESO DEL USUARIO AUTORIZADO Y**, POR OTRO LADO, EVITAR EL ACCESO NO AUTORIZADO A LOS SISTEMAS DE INFORMACIÓN DE LA ORGANIZACIÓN

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

9. CONTROL DE ACCESO

CATEGORÍAS	CONTROLES
9.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO	9.1.1 POLÍTICA DE CONTROL DE ACCESO
	9.1.2 ACCESO A LAS REDES Y A LOS SERVICIOS DE RED
9.2 GESTIÓN DE ACCESO DE USUARIO	9.2.1 REGISTRO Y BAJA DE USUARIO
	9.2.2 PROVISIÓN DE ACCESO DE USUARIO
	9.2.3 GESTIÓN DE PRIVILEGIOS DE ACCESO
	9.2.4 GESTIÓN DE LA INFORMACIÓN SECRETA DE AUTENTICACIÓN DE LOS USUARIOS
	9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIO
	9.2.6 RETIRADA O REASIGNACIÓN DE LOS DERECHOS DE ACCESO

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

9. CONTROL DE ACCESO

CATEGORÍAS	CONTROLES
9.3 RESPONSABILIDADES DEL USUARIO	9.3.1 USO DE LA INFORMACIÓN SECRETA DE AUTENTICACIÓN
9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN
	9.4.2 PROCEDIMIENTOS SEGUROS DE INICIO DE SESIÓN
	9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS
	9.4.4 USO DE UTILIDADES CON PRIVILEGIOS DEL SISTEMA
	9.4.5 CONTROL DE ACCESO AL CÓDIGO FUENTE DE LOS PROGRAMAS

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

10. CRIPTOGRAFÍA

LA ORGANIZACIÓN DEBE GARANTIZAR UN USO ADECUADO Y EFICAZ DE LA CRIPTOGRAFÍA PARA PROTEGER LA CONFIDENCIALIDAD, AUTENTICIDAD Y/O INTEGRIDAD DE LA INFORMACIÓN.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

10. CRIPTOGRAFÍA

CATEGORÍAS	CONTROLES
10.1 CONTROLES CRIPTOGRÁFICOS	10.1.1 POLÍTICA DE USO DE LOS CONTROLES CRIPTOGRÁFICOS
	10.1.2 GESTIÓN DE CLAVES

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

11. SEGURIDAD FÍSICA Y DEL ENTORNO

LOS MEDIOS FÍSICOS DE PROCESAMIENTO DE INFORMACIÓN **DEBEN ESTAR SITUADOS EN ÁREAS SEGURAS**, PROTEGIDAS POR PERÍMETROS DE SEGURIDAD DEFINIDOS, CON BARRERAS DE SEGURIDAD Y CONTROLES DE ENTRADA Y SALIDA APROPIADOS.

LA INFORMACIÓN CRÍTICA Y CONFIDENCIAL DEBE TENER UN MAYOR NIVEL DE PROTECCIÓN FÍSICA ANTE ACCESOS NO AUTORIZADOS Y AMENAZAS FÍSICAS Y AMBIENTALES.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

11. SEGURIDAD FÍSICA Y DEL ENTORNO

CATEGORÍAS	CONTROLES
11.1 ÁREAS SEGURAS	11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA
	11.1.2 CONTROLES FÍSICOS DE ENTRADA
	11.1.3 SEGURIDAD DE OFICINAS, DESPACHOS Y RECURSOS
	11.1.4 PROTECCIÓN CONTRA LAS AMENAZAS EXTERNAS Y AMBIENTALES
	11.1.5 EL TRABAJO EN ÁREAS SEGURAS
	11.1.6 ÁREAS DE CARGA Y DESCARGA

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

11. SEGURIDAD FÍSICA Y DEL ENTORNO

CATEGORÍAS	CONTROLES
11.2 SEGURIDAD DE LOS EQUIPOS	11.2.1 EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS
	11.2.2 INSTALACIONES DE SUMINISTRO
	11.2.3 SEGURIDAD DEL CABLEADO
	11.2.4 MANTENIMIENTO DE LOS EQUIPOS
	11.2.5 RETIRADA DE MATERIALES PROPIEDAD DE LA EMPRESA
	11.2.6 SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES
	11.2.7 REUTILIZACIÓN O ELIMINACIÓN SEGURA DE EQUIPOS
	11.2.8 EQUIPO DE USUARIO DESATENDIDO
	11.2.9 POLÍTICA DE PUESTO DE TRABAJO DESPEJADO Y PANTALLA LIMPIA

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

12. SEGURIDAD DE LAS OPERACIONES

LOS OBJETIVOS SON:

- ASEGURAR EL FUNCIONAMIENTO CORRECTO Y SEGURO DE LAS INSTALACIONES DE TRATAMIENTO DE LA INFORMACIÓN
- ASEGURAR QUE LOS RECURSOS DE TRATAMIENTO DE INFORMACIÓN Y LA INFORMACIÓN ESTÁN PROTEGIDOS CONTRA EL MALWARE
- EVITAR LA PÉRDIDA DE DATOS
- REGISTRAR EVENTOS Y GENERAR EVIDENCIAS
- ASEGURAR LA INTEGRIDAD DEL SOFTWARE EN EXPLOTACIÓN
- REDUCIR LOS RIESGOS RESULTANTES DE LA EXPLOTACIÓN DE LAS VULNERABILIDADES TÉCNICAS
- MINIMIZAR EL IMPACTO DE LAS ACTIVIDADES DE AUDITORÍA EN LOS SISTEMAS OPERATIVOS

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

12. SEGURIDAD DE LAS OPERACIONES

CATEGORÍAS	CONTROLES
12.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES	12.1.1 DOCUMENTACIÓN DE PROCEDIMIENTOS DE OPERACIÓN
	12.1.2 GESTIÓN DE CAMBIOS
	12.1.3 GESTIÓN DE CAPACIDADES
	12.1.4 SEPARACIÓN DE LOS RECURSOS DE DESARROLLO, PRUEBA Y OPERACIÓN
12.2 PROTECCIÓN CONTRA EL SOFTWARE MALICIOSO (MALWARE)	12.2.1 CONTROLES CONTRA EL CÓDIGO MALICIOSO

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

12. SEGURIDAD DE LAS OPERACIONES

CATEGORÍAS	CONTROLES
12.3 COPIAS DE SEGURIDAD	12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN
12.4 REGISTROS Y SUPERVISIÓN	12.4.1 REGISTRO DE EVENTOS
	12.4.2 PROTECCIÓN DE LA INFORMACIÓN DEL REGISTRO
	12.4.3 REGISTROS DE ADMINISTRACIÓN Y OPERACIÓN
	12.4.4 SINCRONIZACIÓN DEL RELOJ

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

12. SEGURIDAD DE LAS OPERACIONES

CATEGORÍAS	CONTROLES
12.5 CONTROL DEL SOFTWARE EN EXPLOTACIÓN	12.5.1 INSTALACIÓN DEL SOFTWARE EN EXPLOTACIÓN
12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA	12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS
	12.6.2 RESTRICCIÓN EN LA INSTALACIÓN DE SOFTWARE
12.7 CONSIDERACIONES SOBRE LA AUDITORIA DE SISTEMAS DE INFORMACIÓN	12.7.1 CONTROLES DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

13. SEGURIDAD DE LAS COMUNICACIONES

LOS OBJETIVOS SON:

- ASEGURAR LA PROTECCIÓN DE LA INFORMACIÓN EN LAS REDES Y LOS RECURSOS DE TRATAMIENTO DE LA INFORMACIÓN
- MANTENER LA SEGURIDAD EN LA INFORMACIÓN QUE SE TRANSFIERE DENTRO DE UNA ORGANIZACIÓN Y CON CUALQUIER ENTIDAD EXTERNA

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

13. SEGURIDAD DE LAS COMUNICACIONES

CATEGORÍAS	CONTROLES
13.1 GESTIÓN DE LA SEGURIDAD DE REDES	13.1.1 CONTROLES DE RED
	13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED
	13.1.3 SEGREGACIÓN EN REDES
13.2 INTERCAMBIO DE INFORMACIÓN	13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACIÓN
	13.2.2 ACUERDOS DE INTERCAMBIO DE INFORMACIÓN
	13.2.3 MENSAJERÍA ELECTRÓNICA
	13.2.4 ACUERDOS DE CONFIDENCIALIDAD O NO REVELACIÓN

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

EL DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE INFORMACIÓN ES VITAL PARA LA SEGURIDAD.

ES NECESARIO GARANTIZAR QUE LA SEGURIDAD SEA UNA PARTE INTEGRAL DE LOS SISTEMAS DE INFORMACIÓN.

ANTES DE DESARROLLAR E IMPLEMENTAR LOS SISTEMAS DE INFORMACIÓN ES NECESARIO IDENTIFICAR Y ACORDAR LOS DISTINTOS REQUERIMIENTOS DE SEGURIDAD DE CADA ÁREA DE LA ORGANIZACIÓN IMPLICADA EN DICHA IMPLEMENTACIÓN.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

CATEGORÍAS	CONTROLES
14.1 REQUISITOS DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN	14.1.1 ANÁLISIS DE REQUISITOS Y ESPECIFICACIONES DE SEGURIDAD DE LA INFORMACIÓN
	14.1.2 ASEGURAR LOS SERVICIOS DE APLICACIONES EN REDES PÚBLICAS
	14.1.3 PROTECCIÓN DE LAS TRANSACCIONES DE SERVICIOS DE APLICACIONES

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

CATEGORÍAS	CONTROLES
14.2 SEGURIDAD EN EL DESARROLLO Y EN LOS PROCESOS DE SOPORTE	14.2.1 POLÍTICA DE DESARROLLO SEGURO
	14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS
	14.2.3 REVISIÓN TÉCNICA DE LAS APLICACIONES TRAS EFECTUAR CAMBIOS EN EL SISTEMA OPERATIVO
	14.2.4 RESTRICCIONES A LOS CAMBIOS EN LOS PAQUETES DE SOFTWARE
	14.2.5 PRINCIPIOS DE INGENIERÍA DE SISTEMAS SEGUROS
	14.2.6 ENTORNO DE DESARROLLO SEGURO
	14.2.7 EXTERNALIZACIÓN DEL DESARROLLO DE SOFTWARE
	14.2.8 PRUEBAS FUNCIONALES DE SEGURIDAD DE SISTEMAS
	14.2.9 PRUEBAS DE ACEPTACIÓN DE SISTEMAS
14.3 DATOS DE PRUEBA	14.3.1 PROTECCIÓN DE LOS DATOS DE PRUEBA

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

15. RELACIÓN CON PROVEEDORES

LOS OBJETIVOS SON:

- ASEGURAR LA PROTECCIÓN DE LOS ACTIVOS DE LA ORGANIZACIÓN QUE SEAN ACCESIBLES A LOS PROVEEDORES
- MANTENER UN NIVEL ACORDADO DE SEGURIDAD Y DE PROVISIÓN DE SERVICIOS EN LÍNEA CON ACUERDOS CON PROVEEDORES

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

15. RELACIÓN CON PROVEEDORES

CATEGORÍAS	CONTROLES
15.1 SEGURIDAD EN LAS RELACIONES CON PROVEEDORES	15.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES
	15.1.2 REQUISITOS DE SEGURIDAD EN CONTRATOS CON TERCEROS
	15.1.3 CADENA DE SUMINISTRO DE TECNOLOGÍA DE LA INFORMACIÓN Y DE LAS COMUNICACIONES
15.2 GESTIÓN DE LA PROVISIÓN DE SERVICIOS DEL PROVEEDOR	15.2.1 CONTROL Y REVISIÓN DE LA PROVISIÓN DE SERVICIOS DEL PROVEEDOR
	15.2.2 GESTIÓN DE CAMBIOS EN LA PROVISIÓN DEL SERVICIO DEL PROVEEDOR

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

CUALQUIER INCIDENTE QUE AFECTE A LA SEGURIDAD DE LA INFORMACIÓN DEBE COMUNICARSE A LOS RESPONSABLES DEL ESTABLECIMIENTO DE LAS MEDIDAS CORRECTIVAS.

SE ESTABLECEN PROCEDIMIENTOS DE REPORTE QUE ESPECIFIQUEN QUÉ HAY QUE COMUNICAR, A QUIÉN, CÓMO Y CUÁNDO HAY QUE HACERLO.

LA IDEA ES QUE LA ORGANIZACIÓN APRENDA DE LOS ERRORES COMETIDOS MEDIANTE LA REALIZACIÓN DE UN SEGUIMIENTO Y SUPERVISIÓN DE CADA INCIDENCIA.

TAMBIÉN SE CONTROLA EL PROCEDIMIENTO DE RESOLUCIÓN DE LAS INCIDENCIAS Y SU RESOLUCIÓN FINAL.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

CATEGORÍAS	CONTROLES
16.1 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS	16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS
	16.1.2 NOTIFICACIÓN DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN
	16.1.3 NOTIFICACIÓN DE PUNTOS DÉBILES DE LA SEGURIDAD
	16.1.4 EVALUACIÓN Y DECISIÓN SOBRE LOS EVENTOS DE SEGURIDAD DE INFORMACIÓN
	16.1.5 RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
	16.1.6 APRENDIZAJE DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
	16.1.7 RECOPILACIÓN DE EVIDENCIAS

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

DEBE TENER INCLUIDA LA SEGURIDAD DE LA INFORMACIÓN, YA QUE CUALQUIER FALLO EN LA SEGURIDAD PUEDE INFLUIR NEGATIVAMENTE EN LA ESTABILIDAD DE LA ORGANIZACIÓN Y LLEGAR A PROVOCAR AUTÉNTICAS DEBACLES.

ES NECESARIO IDENTIFICAR LOS PROCESOS CRÍTICOS QUE AFECTEN A LA CONTINUIDAD DEL NEGOCIO E INTEGRAR EN ELLOS LOS REQUERIMIENTOS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, IMPLANTAR CONTROLES PREVENTIVOS QUE MINIMICEN LOS RIESGOS Y ESTABLECER MEDIDAS QUE PERMITAN CONTINUAR CON LA ACTIVIDAD DE LA ORGANIZACIÓN EN EL MOMENTO EN EL QUE SE PRODUZCA CUALQUIER INCIDENCIA.

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

CATEGORÍAS	CONTROLES
17.1 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN
	17.1.2 IMPLEMENTAR LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN
	17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN
17.2 REDUNDANCIAS	17.2.1 DISPONIBILIDAD DE LOS RECURSOS DE TRATAMIENTO DE LA INFORMACIÓN

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

18. CUMPLIMIENTO

EL OBJETIVO DE ESTE APARTADO CONSISTE EN EVITAR CUALQUIER INCUMPLIMIENTO LEGAL, ESTATUTARIO, REGULADOR O CONTRACTUAL, Y CUALQUIER REQUERIMIENTO DE SEGURIDAD.

SE RECOMIENDA CONSULTAR CON ASESORES Y PROFESIONALES LEGALES CALIFICADOS Y REALIZAR AUDITORÍAS DE LOS SISTEMAS DE INFORMACIÓN DE FORMA PERIÓDICA.

CON ELLO, SE GARANTIZA QUE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ESTÉ ADAPTADA CORRECTAMENTE A LA NORMATIVA VIGENTE

2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

NORMA ISO 27002

18. CUMPLIMIENTO

CATEGORÍAS	CONTROLES
18.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES	18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES
	18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL (DPI)
	18.1.3 PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN
	18.1.4 PROTECCIÓN Y PRIVACIDAD DE LA INFORMACIÓN DE CARÁCTER PERSONAL
	18.1.5 REGULACIÓN DE LOS CONTROLES CRIPTOGRÁFICOS
18.2 REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN	18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN
	18.2.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD
	18.2.3 COMPROBACIÓN DEL CUMPLIMIENTO TÉCNICO

CONTENIDOS

1. INTRODUCCIÓN
2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
3. **METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN**
4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
5. NORMATIVAS MÁS FRECUENTEMENTE UTILIZADAS PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

INTRODUCCIÓN

HASTA HACE POCO **LAS INFRAESTRUCTURAS INFORMÁTICAS SE LIMITABAN A DAR SERVICIOS DE APOYO A OTRAS ÁREAS** CÓMO OTRO MATERIAL DE OFICINA.

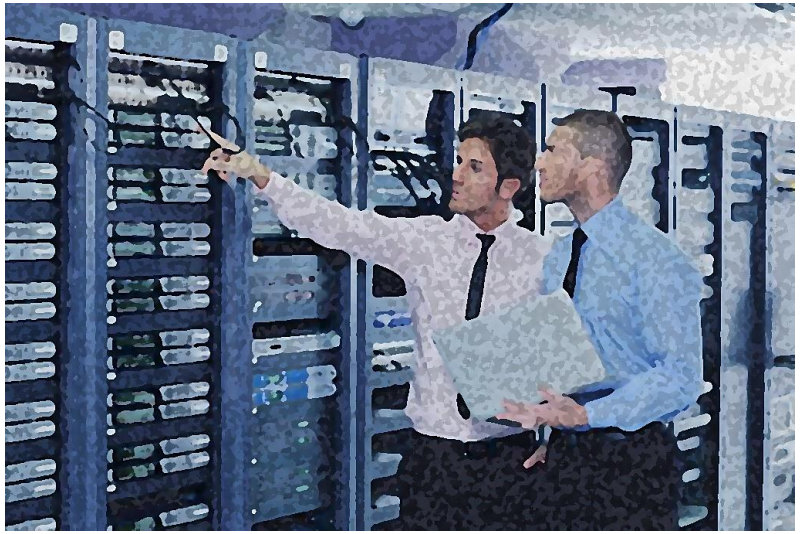
ACTUALMENTE, LOS SERVICIOS TI SON UNA PARTE SUSTANCIAL DE LOS PROCESOS DE NEGOCIO.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

INTRODUCCIÓN

UNA BUENA GESTIÓN DE SERVICIOS **TI** HA DE:

- PROPORCIONAR UNA ADECUADA GESTIÓN DE LA CALIDAD
- AUMENTAR LA EFICIENCIA
- ALINEAR LOS PROCESOS DE NEGOCIO Y LA INFRAESTRUCTURA TI
- REDUCIR LOS RIESGOS ASOCIADOS A LOS SERVICIOS TI
- GENERAR NEGOCIO



3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

INTRODUCCIÓN

ITIL NACE COMO UN ***CÓDIGO DE BUENAS PRÁCTICAS*** DIRIGIDAS A ALCANZAR ESAS METAS MEDIANTE:

- UN ENFOQUE DEL SERVICIO **TI** CENTRADO EN LOS PROCESOS Y PROCEDIMIENTOS
- ESTABLECIMIENTO DE ESTRATEGIAS PARA LA GESTIÓN OPERATIVA DE LA INFRAESTRUCTURA **TI**

ITIL® 4 FOUNDATION

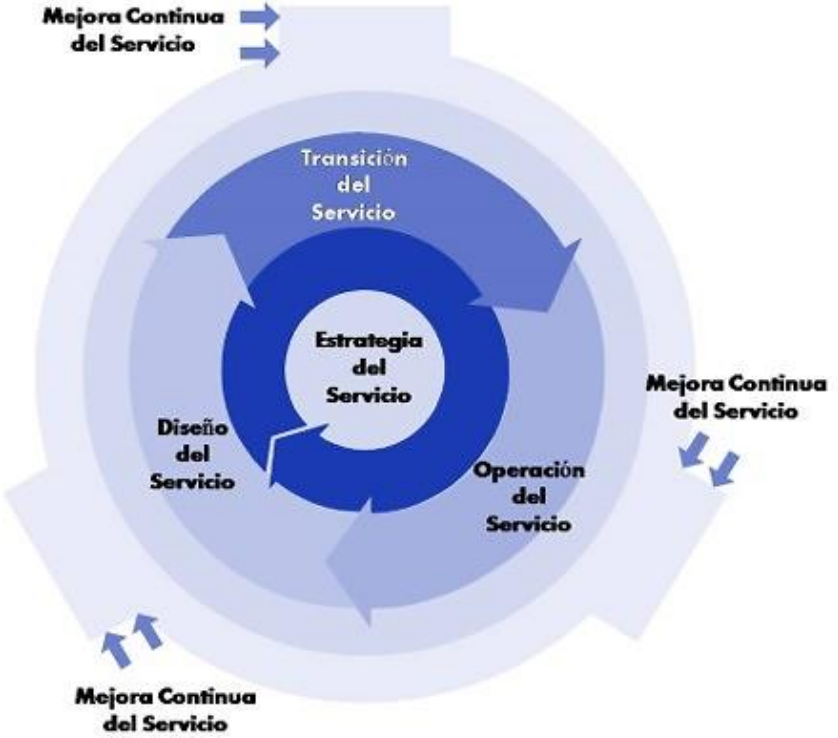
ITIL
Information
Technology
Insfrastructure
Library

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

DESARROLLADA A FINALES DE 1980, **LA BIBLIOTECA DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN (ITIL)** ES EL ESTÁNDAR MUNDIAL EN LA GESTIÓN DE SERVICIOS INFORMÁTICOS

INICIADO COMO UNA GUÍA PARA EL GOBIERNO DE UK, HA DEMOSTRADO SER ÚTIL PARA LAS ORGANIZACIONES A TRAVÉS DE SU ADOPCIÓN POR INNUMERABLES COMPAÑÍAS COMO BASE PARA CONSULTA, EDUCACIÓN Y SOPORTE DE HERRAMIENTAS DE SOFTWARE.



3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

ITIL SE DESARROLLÓ YA QUE **LAS ORGANIZACIONES DEPENDEN CADA VEZ MÁS DE LA INFORMÁTICA** PARA ALCANZAR SUS OBJETIVOS CORPORATIVOS.

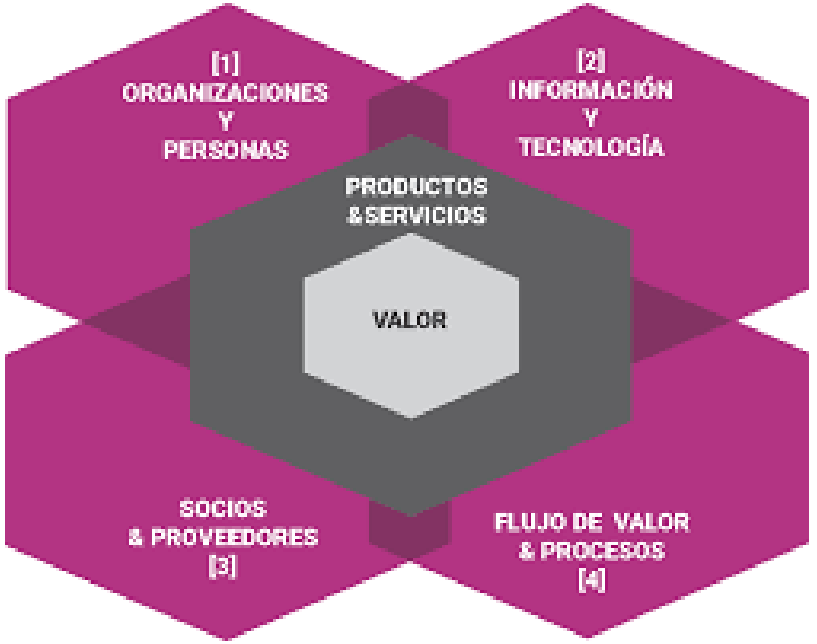
HAY UNA NECESIDAD CRECIENTE DE **SERVICIOS INFORMÁTICOS DE CALIDAD QUE SE CORRESPONDAN CON LOS OBJETIVOS DEL NEGOCIO, Y QUE SATISFAGAN LOS REQUISITOS Y LAS EXPECTATIVAS DEL CLIENTE.**

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

EL ÉNFASIS **HA PASADO DEL DESARROLLO DE LAS APLICACIONES TI A LA GESTIÓN DE SERVICIOS TI**.

LA APLICACIÓN TI SÓLO **CONTRIBUYE A REALIZAR LOS OBJETIVOS CORPORATIVOS SI EL SISTEMA ESTÁ A DISPOSICIÓN DE LOS USUARIOS** Y, ES SOPORTADO POR LOS PROCESOS DE MANTENIMIENTO Y OPERACIONES.



3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL. LA HISTORIA DE ITIL

- **LA DÉCADA DE 1980: EL NACIMIENTO DE ITIL**
- **1990-1999: ITIL V1**

  DESARROLLO INICIAL DE LAS MEJORES PRÁCTICAS PARA LA GESTIÓN DE SERVICIOS DE TI
- **2000-2006: ITIL V2**

  ENFOQUE EN PROCESOS Y FUNCIONES CLAVE. INTRODUCCIÓN DE LIBROS ESPECÍFICOS PARA ÁREAS COMO SOPORTE Y ENTREGA DE SERVICIOS
- **2007-2018: ITIL V3**

  ENFOQUE EN EL CICLO DE VIDA DEL SERVICIO. DIVISIÓN EN 5 LIBROS CENTRADOS EN ESTRATEGIA, DISEÑO, TRANSICIÓN, OPERACIÓN Y MEJORA CONTINUA DEL SERVICIO
- **2019- : ITIL V4**

  ADAPTACIÓN A LA TRANSFORMACIÓN DIGITAL. ENFOQUE EN LA CREACIÓN DE VALOR A TRAVÉS DE SERVICIOS Y EXPERIENCIAS DE USUARIO. INTEGRACIÓN CON PRÁCTICAS ÁGILES, DevOps Y GESTIÓN EN LA NUBE

ES IMPORTANTE DESTACAR QUE **ITIL NO ES UNA NORMA, SINO UN MARCO DE TRABAJO**

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

ITIL ES UN CONJUNTO DE **MEJORES PRÁCTICAS** FORMADO A PARTIR DE LAS **OPINIONES Y EXPERIENCIAS** DE TODA UNA COMUNIDAD DE **TI.**

PROPORCIONA UN MARCO PARA **GESTIONAR TODOS LOS ASPECTOS** DE LA PRESTACIÓN DE SERVICIOS DE **TI,** DESDE LA PLANIFICACIÓN, DESARROLLO Y DESPLIEGUE DE NUEVOS SERVICIOS HASTA LA MEJORA CONTINUA DE LOS EXISTENTES.

AYUDA A GARANTIZAR QUE **TI** OFREZCA VALOR EN LOS SERVICIOS ENTREGADOS Y **SATISFAGA** LAS NECESIDADES DE SUS CLIENTES Y USUARIOS.

EL **OBJETIVO PRINCIPAL DE ITIL ES ALINEAR LOS SERVICIOS DE TI CON LAS NECESIDADES DEL NEGOCIO.**

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CARACTERÍSTICAS DE ITIL

- **VENDOR NEUTRAL**
  ES APLICABLE A CUALQUIER ORGANIZACIÓN QUE BRINDA SERVICIOS DE TI. NO SE BASA EN NINGUNA PLATAFORMA PARTICULAR.
- **SIN PERSPECTIVA**
  APLICA A TODOS OS TIPOS DE ORGANIZACIÓN DE SERVICIOS DE TI
- **MEJORES PRÁCTICAS**
  REPRESENTA LAS EXPERIENCIAS DE APRENDIZAJE Y LIDERAZGO DE PENSAMIENTO DE LOS MEJORES PROVEEDORES DE SERVICIOS DEL MUNDO.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

ES IMPORTANTE QUE HAYA UN **ENTENDIMIENTO DE LA TERMINOLOGÍA DE ITIL PARA SU USO EFECTIVO EN ESCENARIOS REALES** DE GESTIÓN DE SERVICIOS EN LAS ORGANIZACIONES.

VEAMOS, EN PRIMER LUGAR, LA DEFINICIÓN DE GESTIÓN DE SERVICIOS.

GESTIÓN DE SERVICIOS

ES EL CONJUNTO DE CAPACIDADES ESPECIALIZADAS QUE TIENEN LAS ORGANIZACIONES PARA HABILITAR LA ENTREGA DE VALOR A LOS CLIENTES EN FORMA DE SERVICIOS

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

LOS CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS SON:

- **VALOR Y COCREACIÓN DE VALOR**
- **ORGANIZACIÓN, PROVEEDORES DE SERVICIO, CONSUMIDORES DE SERVICIO Y OTROS INTERESADOS**
- **PRODUCTOS Y SERVICIOS**
- **RELACIONES DE SERVICIO**
- **VALOR: RESULTADOS, COSTOS Y RIESGOS**
- **UTILIDAD Y GARANTÍA**

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

VALOR Y COCREACIÓN DE VALOR

VALOR

ES LA UTILIDAD, IMPORTANCIA Y BENEFICIOS PERCIBIDOS DE ALGO. ***EL OBJETIVO DE UNA ORGANIZACIÓN ES CREAR VALOR PARA LAS PARTES INTERESADAS.***

COCREACIÓN DE VALOR

EL VALOR SE LOGRA A TRAVÉS DE LA COLABORACIÓN ACTIVA ENTRE PROVEEDORES Y CLIENTES Y OTRAS PARTES INTERESADAS. TODOS CONTRIBUYEN A DEFINIR LOS REQUISITOS, DISEÑAR SOLUCIONES DE SERVICIO, E INCLUSO A LA CREACIÓN Y/O PRESTACIÓN DEL SERVICIO EN SÍ.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

ORGANIZACIÓN, PROVEEDORES DE SERVICIO, CONSUMIDORES DE SERVICIO Y OTROS INTERESADOS

ORGANIZACIÓN

ES UN GRUPO DE PERSONAS QUE, CON SUS PROPIAS FUNCIONES, RESPONSABILIDADES, AUTORIDAD Y RELACIONES, ALCANZAN SUS OBJETIVOS.

PROVEEDOR DE SERVICIOS

ES UN ROL DESARROLLADO DENTRO DE UNA ORGANIZACIÓN QUE PROPORCIONA SERVICIOS A LOS CONSUMIDORES EN UNA RELACIÓN DE SERVICIOS. DEBE TENER CLARO QUIÉN ES EL CONSUMIDOR Y QUE OTROS INTERESADOS PARTICIPAN EN LA RELACIÓN DE SERVICIO.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

ORGANIZACIÓN, PROVEEDORES DE SERVICIO, CONSUMIDORES DE SERVICIO Y OTROS INTERESADOS

CONSUMIDOR DE SERVICIOS

ES UN ROL GENÉRICO UTILIZADO PARA SIMPLIFICAR A DEFINICIÓN Y DESCRIPCIÓN DE INVOLUCRADOS EN UNA RELACIÓN DE SERVICIO:

- **CLIENTE:** PERSONA QUE DEFINE LOS REQUERIMIENTOS DE UN SERVICIO
- **USUARIO:** PERSONA QUE USA EL SERVICIO
- **PATROCINADOR:** PERSONA QUE AUTORIZA EL PRESUPUESTO PARA EL CONSUMO DEL SERVICIO

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

ORGANIZACIÓN, PROVEEDORES DE SERVICIO, CONSUMIDORES DE SERVICIO Y OTROS INTERESADOS

INTERESADOS (STAKEHOLDERS)

PERSONA U ORGANIZACIÓN QUE TIENE ALGÚN INTERÉS EN UNA ORGANIZACIÓN, PRODUCTO, SERVICIO, PRÁCTICA O ENTIDAD.

Interesado (stakeholder)	Ejemplo de valor esperado
Consumidor de servicios	Beneficios alcanzados; costos y riesgos optimizados.
Proveedor de servicio	Fondos provenientes del cliente; desarrollo de negocio; mejora de imagen pública.
Empleados del proveedor de servicio	Incentivos financieros y no financieros; desarrollo de carrera profesional; sentido de propósito vital.
Sociedad y comunidad	Empleo, impuestos, contribución de las organizaciones al desarrollo de la comunidad.
Organizaciones de caridad	Contribuciones financieras y no financieras.
Accionista (*shareholder*)	Beneficios financieros (dividendos); sensación de seguridad y estabilidad.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

PRODUCTOS Y SERVICIOS

SERVICIO

ES UN MEDIO PARA HABILITAR LA COCREACIÓN DE VALOR, FACILITANDO LOS RESULTADOS QUE EL CLIENTE ESPERA ALCANZAR SIN TENER QUE TRATAR CON LOS COSTOS Y RIESGOS.

PRODUCTO

ES UNA CONFIGURACIÓN DE RECURSOS DE UNA ORGANIZACIÓN DISEÑADA PARA OFRECER VALOR A UN CONSUMIDOR.

LOS SERVICIOS QUE PROPORCIONA UNA ORGANIZACIÓN ESTÁN BASADOS EN UNO O MÁS DE SUS PRODUCTOS.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

PRODUCTOS Y SERVICIOS

OFERTA DE SERVICIO

ES UNA DESCRIPCIÓN FORMAL DE UNO O MÁS SERVICIOS, DISEÑADOS PARA ATENDER LAS NECESIDADES DE UN GRUPO DE CONSUMIDORES OBJETIVO.

Componente	Descripción	Ejemplo
Bienes	Son proporcionados al consumidor. La propiedad de la cosa es transferida al consumidor. El consumidor es responsable de su uso futuro.	Teléfono móvil. Un equipo servidor'físico.
Acceso a recursos	La propiedad no es trasferida al consumidor. La disponibilidad de los recursos está acordada bajo ciertos términos y condiciones. Los consumidores solo pueden tener acceso durante el periodo y en la forma en que fue acordado.	Acceso a la red de datos. Almacenamiento en la nube.
Acciones de servicio	Son desarrolladas o ejecutadas por el proveedor de servicio, para satisfacer las necesidades del consumidor. Se desarrolla respetando lo que se haya acordado entre el consumidor y el proveedor de servicio.	Soporte a usuario. Garantía de equipos.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

RELACIONES DE SERVICIO

RELACIÓN DE SERVICIO

ES LA COOPERACIÓN EXISTENTE ENTRE UN PROVEEDOR DE SERVICIOS Y UN CONSUMIDOR DE SERVICIOS.

UNA RELACIÓN DE SERVICIOS INCLUYE:

- **PROVISIÓN DEL SERVICIO (ENTREGA)**
- **CONSUMO DEL SERVICIO**
- **GESTIÓN DE LA RELACIÓN DEL SERVICIO**

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

RELACIONES DE SERVICIO

RELACIÓN DE SERVICIO

PROVISIÓN DEL SERVICIO

SON LAS ACTIVIDADES DESARROLLADAS POR UNA ORGANIZACIÓN PARA PROPORCIONAR UN SERVICIO. INCLUYE:

- GESTIÓN DE LOS RECURSOS PARA ENTREGAR EL SERVICIO
- ASEGURAR EL ACCESO A LOS RECURSOS AL USUARIO
- CUMPLIMIENTO DE LAS ACCIONES COMPROMETIDAS
- ACUERDO DE NIVEL DE SERVICIO Y MEJORA CONTINUA
- EN OCASIONES, ENTREGA DE BIENES

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

RELACIONES DE SERVICIO

RELACIÓN DE SERVICIO

CONSUMO DEL SERVICIO

SON LAS ACTIVIDADES DESARROLLADAS POR UNA ORGANIZACIÓN PARA CONSUMIR UN SERVICIO. INCLUYE:

- GESTIÓN DE LOS RECURSOS QUE REQUIERE PARA CONSUMIR EL SERVICIO
- EJECUCIÓN DE LAS ACCIONES DE SERVICIO
- ACUERDO DE NIVEL DE SERVICIO Y MEJORA CONTINUA
- EN OCASIONES, RECEPCIÓN DE BIENES

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

RELACIONES DE SERVICIO

GESTIÓN DE LA RELACIÓN DEL SERVICIO

SON LAS ACTIVIDADES CONJUNTAS DESARROLLADAS POR UN PROVEEDOR DE SERVICIO Y UN CONSUMIDOR DE SERVICIO PARA ASEGURAR LA CONTINUA COCREACIÓN DE VALOR BASADOS EN LAS OFERTAS DE SERVICIO ACORDADAS Y DISPONIBLES.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

RELACIONES DE SERVICIO

VALOR: RESULTADOS, COSTOS Y RIESGOS

ALCANZAR LOS RESULTADOS DESEADOS REQUIERE RECURSOS Y REGULARMENTE HAY **COSTOS Y RIESGOS** ASOCIADOS.

SALIDA

ES EL ENTREGABLE (TANGIBLE O INTANGIBLE) DE UNA ACTIVIDAD

RESULTADO

ES UN RESULTADO ENTREGADO A UN INTERESADO A TRAVÉS DE UNA O MÁS SALIDAS

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

RELACIONES DE SERVICIO

VALOR: RESULTADOS, COSTOS Y RIESGOS

COSTO

ES LA CANTIDAD DE DINERO QUE SE GASTA EN UNA ACTIVIDAD O RECURSO.

COSTOS ELIMINADOS

SON LOS COSTOS QUE SE ELIMINAN PARA EL CONSUMIDOR DEL SERVICIO

COSTOS IMPUESTOS

SON LOS COSTOS DERIVADOS A CARGO DEL CONSUMIDOR POR CONSUMIR EL SERVICIO

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

RELACIONES DE SERVICIO

VALOR: RESULTADOS, COSTOS Y RIESGOS

RIESGO

ES EL EVENTO POSIBLE QUE PUEDE CAUSAR DAÑO O PÉRDIDA O QUE PUEDE DIFICULTAR EL LOGRO DE LOS OBJETIVOS.

RIESGOS ELIMINADOS

SON LOS RIESGOS QUE SE ELIMINAN PARA EL CONSUMIDOR DEL SERVICIO

RIESGOS IMPUESTOS

SON LOS RIESGOS ASUMIDOS POR EL CONSUMIDOR POR CONSUMIR EL SERVICIO

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

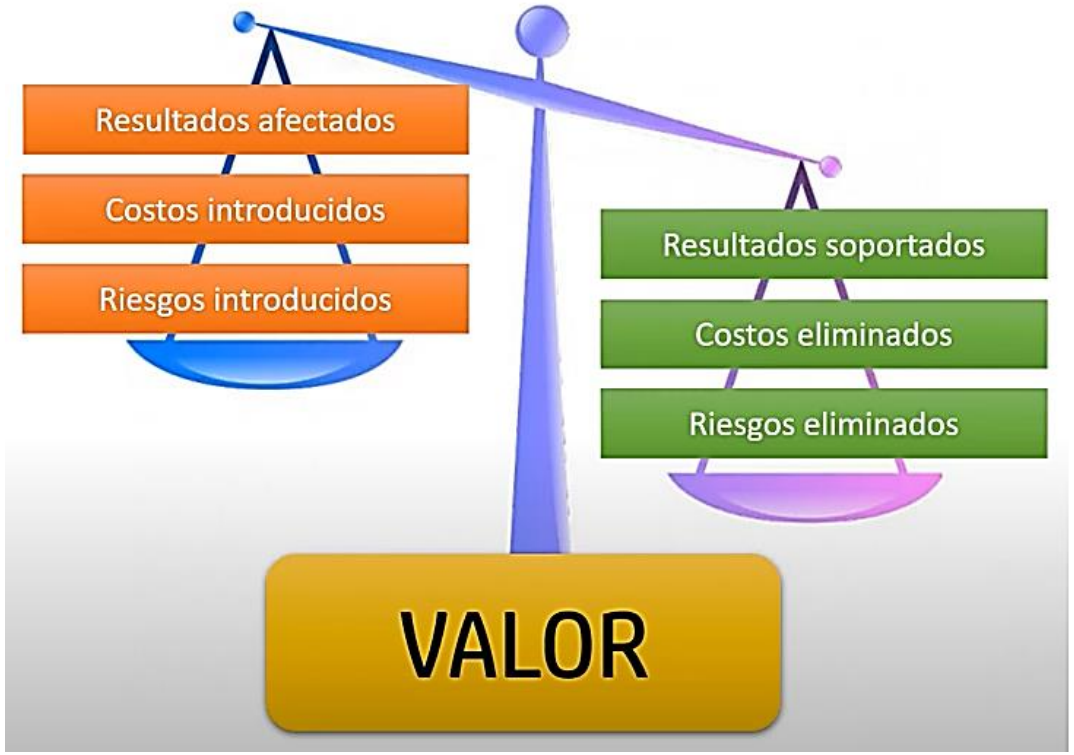
METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

RELACIONES DE SERVICIO

VALOR: RESULTADOS, COSTOS Y RIESGOS

LAS RELACIONES DE SERVICIO SON PERCIBIDAS COMO VALIOSAS CUANDO SUS EFECTOS POSITIVOS SON MAYORES QUE LOS EFECTOS NEGATIVOS



3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

RELACIONES DE SERVICIO

UTILIDAD Y GARANTÍA

UTILIDAD

ES LA FUNCIONALIDAD OFRECIDA POR UN PRODUCTO O SERVICIO Y QUE CONTRIBUYE A SATISFACER UNA NECESIDAD PARTICULAR

GARANTÍA

ES EL GRADO DE SEGURIDAD CON QUE UN PRODUCTO O SERVICIO CUMPLE CON SUS REQUERIMIENTOS ACORDADOS

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CONCEPTOS CLAVE DE LA GESTIÓN DE SERVICIOS

RELACIONES DE SERVICIO

UTILIDAD Y GARANTÍA

NIVEL DE SERVICIO

UNA O MÁS MÉTRICAS QUE DEFINEN LA CALIDAD ESPERADA O ALCANZADA POR UN SERVICIO

DISPONIBILIDAD

ES LA HABILIDAD DE UN SERVICIO DE DESEMPEÑAR SU FUNCIONALIDAD COMPROMETIDA CUANDO ES REQUERIDO

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

ITIL SE COMPONE DE LAS SIGUIENTES PARTES:

- **PRINCIPIOS GUÍA DE ITIL**
- **MODELO DE 4 DIMENSIONES**
- **SISTEMA DE VALOR DEL SERVICIO (SVS)**
- **CADENA DE VALOR DEL SERVICIO (SVC)**

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

PRINCIPIOS GUÍA DE ITIL

SON **7 RECOMENDACIONES** QUE ORIENTAN A UNA ORGANIZACIÓN Y A TODOS SUS INTEGRANTES EN DIFERENTES CIRCUNSTANCIAS. **SON CONSEJOS QUE AYUDAN A ELEGIR ACCIONES Y TOMAR BUENAS DECISIONES** DE TODO TIPO. SON UNIVERSALES Y PERDURABLES:

- **ENFOCARSE EN EL VALOR**
- **EMPEZAR DESDE DONDE ESTEMOS**
- **AVANZAR ITERATIVAMENTE Y CON RETROALIMENTACIÓN**
- **COLABORAR Y PROMOVER LA VISIBILIDAD**
- **PENSAR Y TRABAJAR DE MANERA HOLÍSTICA**
- **MANTENERLO SIMPLE Y PRÁCTICO**
- **OPTIMIZAR Y AUTOMATIZAR**

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

PRINCIPIOS GUÍA DE ITIL

ENFOCARSE EN EL VALOR

TODAS LAS ACTIVIDADES REALIZADAS POR LA ORGANIZACIÓN DEBERÍAN QUEDAR VINCULADAS DE FORMA DIRECTA O INDIRECTA **CON EL VALOR EN SÍ**, SUS CLIENTES Y OTRAS PARTES INTERESADAS.

CONOZCA LA MANERA EN QUE LOS CONSUMIDORES UTILIZAN CADA UNO DE SUS SERVICIOS.

ANIME A TODO EL PERSONAL A QUE SITÚEN EL FOCO DE ATENCIÓN EL VALOR Y SITÚE EL FOCO EN EL VALOR DURANTE LAS ACTIVIDADES COTIDIANAS, ASÍ COMO EN LAS INICIATIVAS DE MEJORA.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

PRINCIPIOS GUÍA DE ITIL

EMPEZAR DESDE DONDE ESTEMOS

APROVECHAR LOS RECURSOS DISPONIBLES PARA LOGRAR UN RESULTADO, EN LUGAR DE INICIAR DESDE CERO.

NO EMPIECE DESDE CERO SIN CONSIDERAR LO QUE YA ESTÁ DISPONIBLE Y QUE SE PUEDE APROVECHAR.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

PRINCIPIOS GUÍA DE ITIL

AVANZAR ITERATIVAMENTE Y CON RETROALIMENTACIÓN

SI ORGANIZA EL TRABAJO EN SECCIONES MÁS PEQUEÑAS Y GESTIONABLES QUE PUEDAN EJECUTARSE Y COMPLETARSE A TIEMPO, **EL ENFOQUE DE CADA ESFUERZO SERÁ MÁS CERTERO Y FÁCIL DE MANTENER**

ITIL 4 TOMA COMO BASE LAS **METODOLOGÍAS ÁGILES** COMO **SCRUM,** USANDO EL **SPRINT**, QUE DESARROLLA CADA UNO DE LOS COMPONENTES Y A PARTIR DE LOS CUALES EL **SCRUM TEAM** RECIBE COMENTARIOS POR PARTE DEL CLIENTE QUE SATISFAGAN SUS NECESIDADES.

ITIL SUGIERE QUE **LA EMPRESA AVANCE JUNTO CON SUS CLIENTES DURANTE EL DESARROLLO DE LOS SERVICIOS E INTERACTÚE CON ELLOS.**

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

PRINCIPIOS GUÍA DE ITIL

COLABORAR Y PROMOVER LA VISIBILIDAD

LOS OBJETIVOS ORGANIZACIONALES SE ALCANZAN CON EL **TRABAJO COLABORATIVO** Y REQUIERE COMPRENSIÓN DEL ENTORNO Y SUS CIRCUNSTANCIAS; ASÍ COMO CONFIANZA Y COMUNICACIÓN EFECTIVA ENTRE LOS INTEGRANTES DE LA ORGANIZACIÓN**, PROPICIANDO LA VISIBILIDAD DEL TRABAJO Y LOS RESULTADOS**.

LA COOPERACIÓN Y LA COLABORACIÓN SON MEJORES QUE EL TRABAJO AISLADO.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

PRINCIPIOS GUÍA DE ITIL

PENSAR Y TRABAJAR HOLÍSTICAMENTE

NINGUNA ACTIVIDAD DENTRO DE LA EMPRESA SUCEDE DE MANERA ESPONTÁNEA Y NO ES REALIZADA POR UNA SOLA PERSONA, SINO QUE ES PRODUCTO DEL TRABAJO COLABORATIVO.

TODAS LAS ÁREAS DEBEN ESTAR INTERCONECTADAS CON EL FIN DE QUE LOS PROCESOS INTERNOS SE LLEVEN A CABO DE FORMA EFICIENTE Y EFICAZ.

LA HOLÍSTICA ES UNA CORRIENTE DEL PENSAMIENTO QUE CONSIDERA A **LOS SISTEMAS COMO ENTES QUE SON MÁS QUE LA SUMA DE SUS PARTES**

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

PRINCIPIOS GUÍA DE ITIL

MANTENERLO SIMPLE Y PRÁCTICO

ES RECOMENDABLE QUE, DURANTE EL DISEÑO DE LOS SERVICIOS, ÉSTOS SE DISEÑEN DE LA MANERA MÁS SENCILLA POSIBLE.

LOS DISEÑOS Y PROCESOS DEBERÁN EVITAR LA COMPLEJIDAD Y MOSTRAR LA PRACTICIDAD CON RESPECTO A LA INTERACCIÓN CON LAS ORGANIZACIONES Y CLIENTES.

SIEMPRE DEBEREMOS UTILIZAR EL MÍNIMO DE PASOS PARA LOGRAR UN OBJETIVO.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

PRINCIPIOS GUÍA DE ITIL

OPTIMIZAR Y AUTOMATIZAR

LA ENTREGA DE SERVICIOS **TI DEBE TENER UN ENFOQUE TOTAL ORIENTADO A LA AUTOMATIZACIÓN.** CUALQUIER PROCESO O PROCEDIMIENTO REPETITIVO ES SUJETO DE AUTOMATIZACIÓN.

COMPRENDER LA VISIÓN Y LOS OBJETIVOS DE LA ORGANIZACIÓN ES EL PRIMER PASO ANTES DE OPTIMIZAR.

- **OPTIMIZAR** ES EL PROCESO DE MEJORAR Y AUMENTAR LA EFICIENCIA DE UN PROCESO O SERVICIO.
- **AUTOMATIZAR** ES USAR LA TECNOLOGÍA PARA REALIZAR UNA SERIE DE PASOS DE MANERA CORRECTA Y CONSISTENTE CON UNA PARTICIPACIÓN HUMANA LIMITADA O NULA.

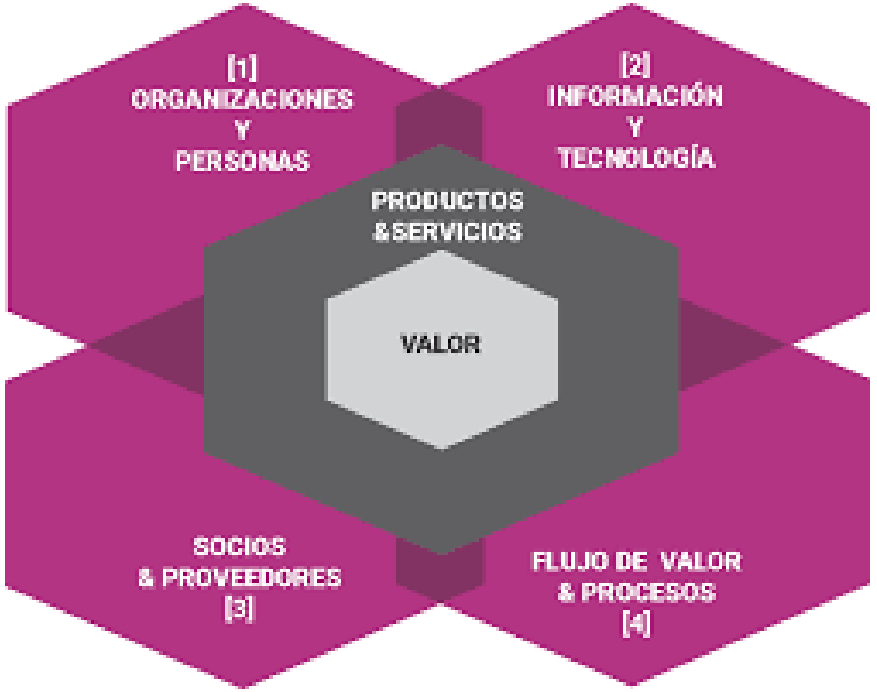
3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

MODELO DE 4 DIMENSIONES

CADA ELEMENTO DEL SISTEMA DE VALOR DEL SERVICIO (SVS) DE VE AFECTADO POR 4 DIMENSIONES

- **LAS ORGANIZACIONES Y LAS PERSONAS**
- **INFORMACIÓN Y TECNOLOGÍA**
- **SOCIOS Y PROVEEDORES**
- **FLUJO DE VALOR Y PROCESOS**



3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

MODELO DE 4 DIMENSIONES

LAS ORGANIZACIONES Y LAS PERSONAS

SE DEBE INVOLUCRAR:

- LA ESTRUCTURA Y ADMINISTRACIÓN
- EL NIVEL ADECUADO DE CAPACITACIÓN
- COMPETENCIAS DEL PERSONAL
- ROLES Y RESPONSABILIDADES
- CULTURA ORGANIZACIONAL

TENER LÍNEAS DE MANDO BIEN DEFINIDAS ES LA CLAVE PARA ESTABLECER UNA ORGANIZACIÓN BIEN ESTRUCTURADA, LO QUE AYUDA A PRESTAR SERVICIOS EFICIENTES.

LAS PERSONAS SON EL ACTIVO MÁS IMPORTANTE DE CUALQUIER ORGANIZACIÓN. AUNQUE HAYA TECNOLOGÍA Y MÁQUINAS, CONTAR CON LAS PERSONAS ADECUADAS EN LOS LUGARES INDICADOS PUEDE TENER UN VALOR INCALCULABLE.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

MODELO DE 4 DIMENSIONES

INFORMACIÓN Y TECNOLOGÍA

LA GESTIÓN DE LA INFORMACIÓN ES EL PRINCIPAL MEDIO PARA PERMITIR VALOR AL CLIENTE. LAS TECNOLOGÍAS ESPECÍFICAS DEPENDEN DE LA NATURALEZA DE LOS SERVICIOS QUE SE BRINDAN.

LOS CRITERIOS DE LA INFORMACIÓN SON: **DISPONIBILIDAD, CONFIABILIDAD, ACCESIBILIDAD, ACTUALIDAD, EXACTITUD Y RELEVANCIA.**

ABARCA LAS TECNOLOGÍAS PARA LA GESTIÓN DEL SERVICIO, LOS SISTEMAS DE GESTIÓN DEL FLUJO DE TRABAJO, LOS INVENTARIOS, LAS BASES DE CONOCIMIENTO, LAS HERRAMIENTAS ANALÍTICAS Y LOS SISTEMAS DE COMUNICACIÓN.

ADEMÁS, INCLUYE TODA LA INFORMACIÓN CREADA, ALMACENADA, GESTIONADA Y UTILIZADA POR LA ORGANIZACIÓN DURANTE LA PRESTACIÓN DEL SERVICIO DE TI.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

MODELO DE 4 DIMENSIONES

SOCIOS Y PROVEEDORES

CADA ORGANIZACIÓN Y CADA SERVICIO DEPENDEN DE OTRAS ORGANIZACIONES. LAS RELACIONES ENTRE LAS ORGANIZACIONES INVOLUCRAN VARIOS NIVELES DE INTEGRACIÓN Y FORMALIDAD.

LA ESTRATEGIA DE UNA ORGANIZACIÓN CUANDO SE TRATA DE UTILIZAR SOCIOS Y PROVEEDORES DEBE SER BASADA EN SUS OBJETIVOS, CULTURA Y ENTORNO EMPRESARIAL.

NINGÚN ECOSISTEMA DE GESTIÓN DE SERVICIOS ESTÁ COMPLETO SIN LOS SOCIOS Y PROVEEDORES.

TODA LA ORGANIZACIÓN DEPENDE DE ELLOS PARA LA PRESTACIÓN DE SUS SERVICIOS.

ESTA DIMENSIÓN LAS RELACIONES DE UNA ORGANIZACIÓN CON OTRAS ORGANIZACIONES O INDIVIDUOS QUE PARTICIPAN EN EL DISEÑO, EL DESARROLLO, LA ENTREGA Y EL SOPORTE DE LOS SERVICIOS.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

MODELO DE 4 DIMENSIONES

FLUJO DE VALOR Y PROCESOS

LA ESTRUCTURACIÓN DE LAS ACTIVIDADES EN **FLUJOS DE VALOR** PERMITE TENER UNA IMAGEN CLARA DE LO QUE SE OFRECE Y COMO REALIZAR MEJORAS CONTINUAS EN SUS SERVICIOS.

LOS PROCESOS PUEDEN MEJORAR LA PRODUCTIVIDAD DENTRO DE LAS ORGANIZACIONES. CONTIENEN **PROCEDIMIENTOS** E **INSTRUCCIONES DE TRABAJO** QUE EXPLICAN CÓMO SE LLEVAN A CABO.

CONSISTE EN DEFINIR LAS ACTIVIDADES, LOS FLUJOS DE TRABAJO, LOS PROCESOS Y LOS PROCEDIMIENTOS NECESARIOS PARA ALCANZAR LOS OBJETIVOS EMPRESARIALES ACORDADOS, ADEMÁS DE DETERMINAR CÓMO LOS DIFERENTES INTEGRANTES DE LA ORGANIZACIÓN SE UNEN Y TRABAJAN DE FORMA CONJUNTA PARA HACER POSIBLE LA CREACIÓN DE VALOR A TRAVÉS DE PRODUCTOS Y SERVICIOS.

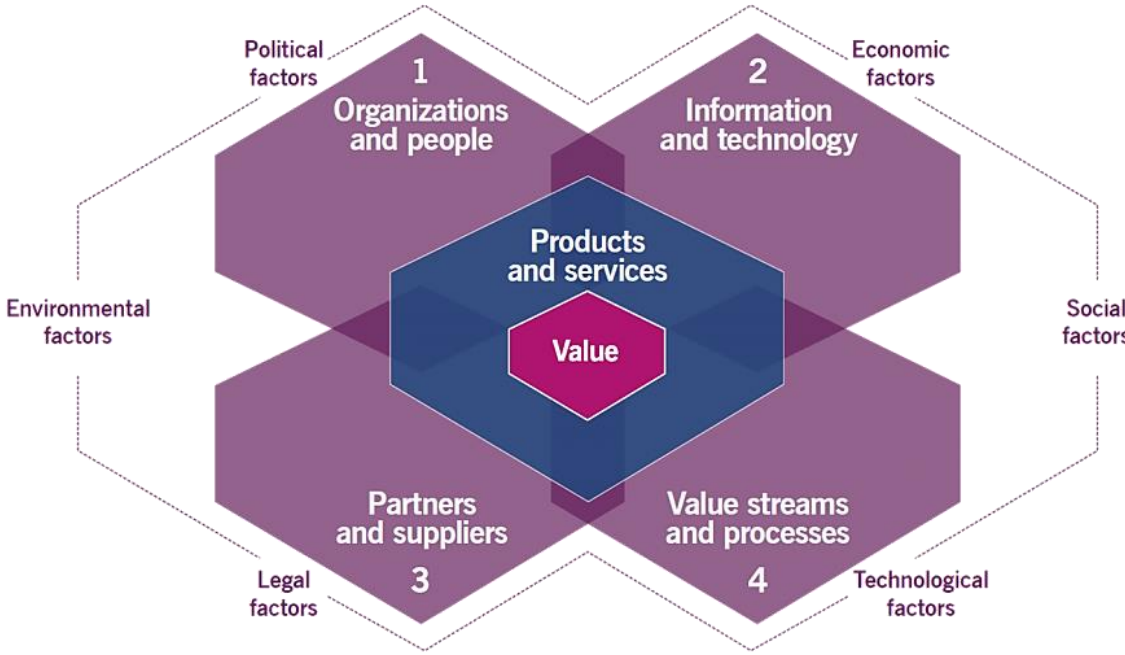
3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

MODELO DE 4 DIMENSIONES

ADEMÁS, CADA DIMENSIÓN ES AFECTADA POR MÚLTIPLES FACTORES:

- **FACTORES POLÍTICOS**
- **FACTORES ECONÓMICOS**
- **FACTORES TECNOLÓGICOS**
- **FACTORES LEGALES**
- **FACTORES AMBIENTALES**
- **FACTORES SOCIALES**



3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

SISTEMA DE VALOR DEL SERVICIO (SVS)

EL **SISTEMA DE VALOR DEL SERVICIO (SVS)** SON **CINCO ACTIVIDADES** INTERCONECTADAS QUE SE INICIAN CUANDO UNA ORGANIZACIÓN TIENE UNA OPORTUNIDAD DE NEGOCIO O DEMANDA DE SERVICIO Y CONCLUYEN CON LA GENERACIÓN DE VALOR.

EL **SVS** TIENE DOS OBJETIVOS PRINCIPALES:

- SE PROMUEVE LA **FLEXIBILIDAD**
- SE PROMUEVE LA **COLABORACIÓN**

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

SISTEMA DE VALOR DEL SERVICIO (SVS)

¿DE DÓNDE SURGE UNA OPORTUNIDAD DE NEGOCIO?

- A PARTIR DE LAS **DEMANDAS DEL CLIENTE**: SOLICITUD DE UN DETERMINADO CLIENTE PARA RESOLVER UNA DETERMINADA SITUACIÓN O PROBLEMÁTICA IDENTIFICADA.
- A PARTIR DE LAS **NECESIDADES CREADAS POR UN PROVEEDOR**: SUCEDE CUANDO EL PROVEEDOR CREA UN SERVICIO QUE LE RESULTA ÚTIL O ATRACTIVO AL CLIENTE Y LO ADQUIERE.

AMBOS SON PUNTOS DE ENTRADA DEL **SVS**, PERO EL PUNTO DE SALIDA ES EL MISMO: **GENERAR VALOR AL CLIENTE A TRAVÉS DE LA CREACIÓN DE SERVICIOS**

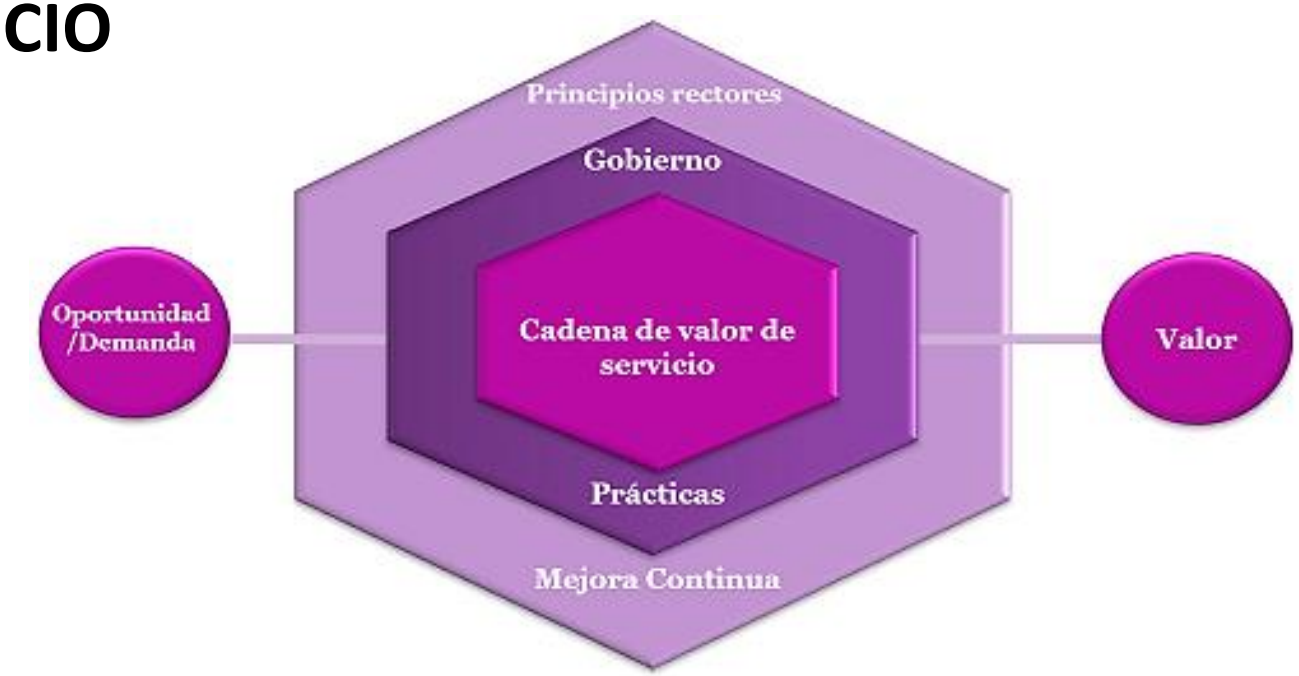
3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

SISTEMA DE VALOR DEL SERVICIO (SVS)

LAS CINCO ACTIVIDADES SON:

- **PRINCIPIOS GUÍA**
- **GOBERNANZA**
- **CADENA DE VALOR DEL SERVICIO**
- **PRÁCTICAS DE GESTIÓN**
- **MEJORA CONTINUA**

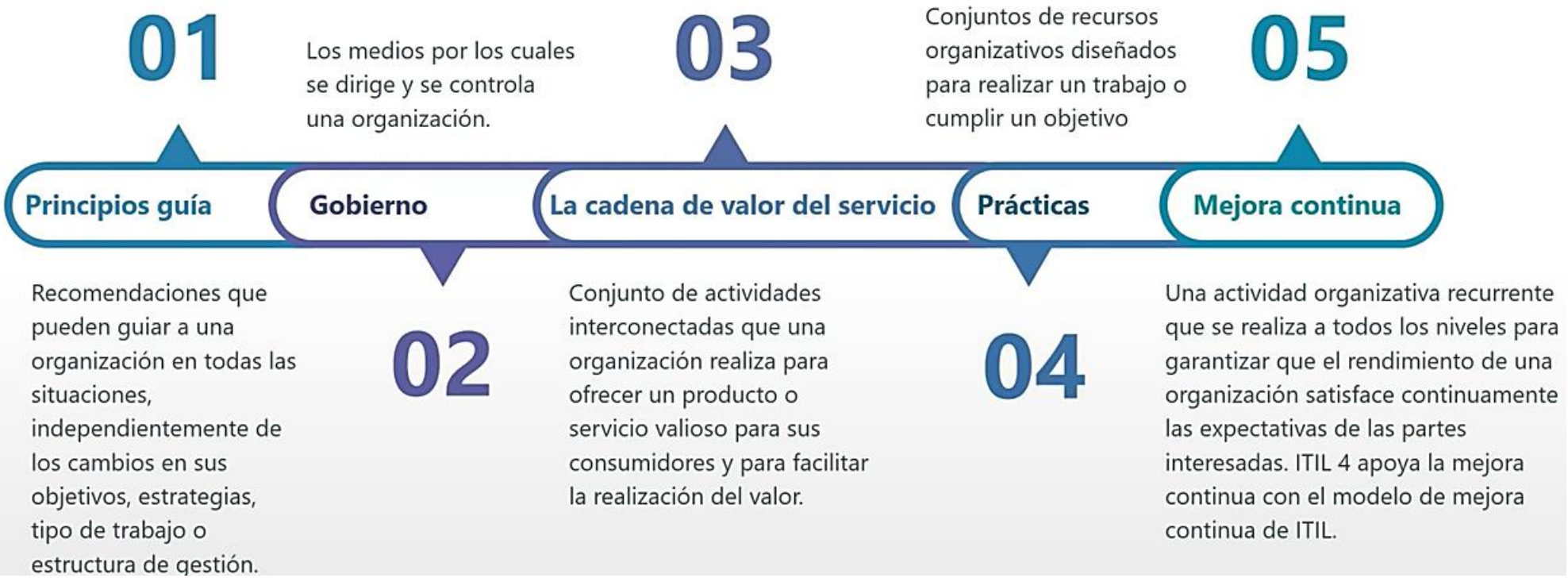


3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

SISTEMA DE VALOR DEL SERVICIO (SVS)

Las entradas clave del SVS son la oportunidad y la demanda. El SVS de ITIL incluye los siguientes elementos:



3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

GOBERNANZA

LA **GOBERNANZA** INCLUYE ACTIVIDADES DE EVALUACIÓN, DIRECCIÓN Y SUPERVISIÓN CON EL OBJETIVO FINAL DE GARANTIZAR QUE LA *CADENA DE VALOR DEL SERVICIO* Y LAS *PRÁCTICAS* DE LA ORGANIZACIÓN FUNCIONEN ALINEADAS CON LOS OBJETIVOS DE LA EMPRESA.

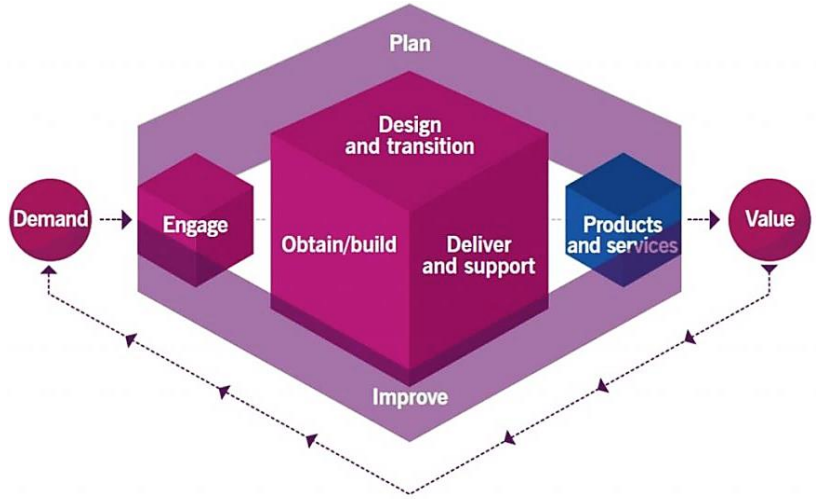
3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

LA CADENA DE VALOR DEL SERVICIO

CONSTA DE 6 ACTIVIDADES INTERRELACIONADAS QUE HACEN USO DE LOS RECURSOS DE LA ORGANIZACIÓN, ORGANIZADOS EN PRÁCTICAS **PARA CREAR Y MEJORAR FLUJOS DE VALOR**, SON:

- **PLANEAR**
- **MEJORAR**
- **INVOLUCRAR**
- **DISEÑO Y TRANSICIÓN**
- **OBTENER/CONSTRUIR**
- **ENTREGA Y SOPORTE**



3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

PRÁCTICAS DE GESTIÓN

SE DEFINEN COMO **UN CONJUNTO DE RECURSOS ORGANIZATIVOS DISEÑADOS PARA REALIZAR UN TRABAJO O ALCANZAR UN OBJETIVO**.

EL NUEVO SISTEMA DE VALOR DE SERVICIOS (SVS) DE **ITIL 4** INCLUYE **34 PRÁCTICAS**, AGRUPADAS EN **3 GRUPOS**:

- **14** PRÁCTICAS DE GESTIÓN **GENERAL**
- **17** PRÁCTICAS DE GESTIÓN **DE SERVICIOS**
- **3** PRÁCTICAS DE GESTIÓN **TÉCNICA**

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

PRÁCTICAS DE GESTIÓN

CADA UNA DE LAS 34 PRÁCTICAS ESTÁ **BASADA EN CUATRO DIMENSIONES** , Y CADA UNA DE ESTAS **AFECTADA POR DISTINTOS FACTORES** (LEGALES, AMBIENTALES, ECONÓMICOS, TECNOLÓGICOS, SOCIALES Y POLÍTICOS).

LAS CUATRO DIMENSIONES SON:

1. ORGANIZACIÓN Y GENTE
2. INFORMACIÓN Y TECNOLOGÍA
3. PROVEEDORES Y ASOCIADOS
4. FLUJOS DE VALOR Y PROCESOS

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

PRÁCTICAS DE GESTIÓN

PRÁCTICAS GENERALES DE GESTIÓN

1. Gestión de arquitectura
2. Mejora continua
3. Gestión de seguridad de la información
4. Gestión del conocimiento
5. Medición y notificación
6. Gestión del cambio organizacional
7. Gestión de la cartera
8. Gestión de proyectos
9. Gestión de las relaciones
10. Gestión de los riesgos
11. Gestión financiera de los servicios
12. Gestión de la estrategia
13. Gestión de los suministros
14. Gestión de la fuerza de trabajo y del talento

PRÁCTICAS DE GESTIÓN DE SERVICIOS

1. Gestión de la disponibilidad
2. Análisis del negocio
3. Gestión de la capacidad y el rendimiento
4. Control de cambios
5. Gestión de incidentes
6. Gestión de activos TI
7. Monitoreo y gestión de eventos
8. Gestión de problemas
9. Gestión de versiones
10. Gestión del catálogo de servicios
11. Gestión de la configuración de servicios
12. Gestión de la continuidad de servicios
13. Diseño del servicio
14. Servicio de atención al cliente
15. Gestión del nivel de servicio
16. Gestión de peticiones de servicio
17. Validación y prueba del servicio

PRÁCTICAS DE GESTIÓN TÉCNICA

1. Gestión de la implementación
2. Gestión de infraestructura y plataformas
3. Desarrollo y gestión del software

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

MEJORA CONTINUA

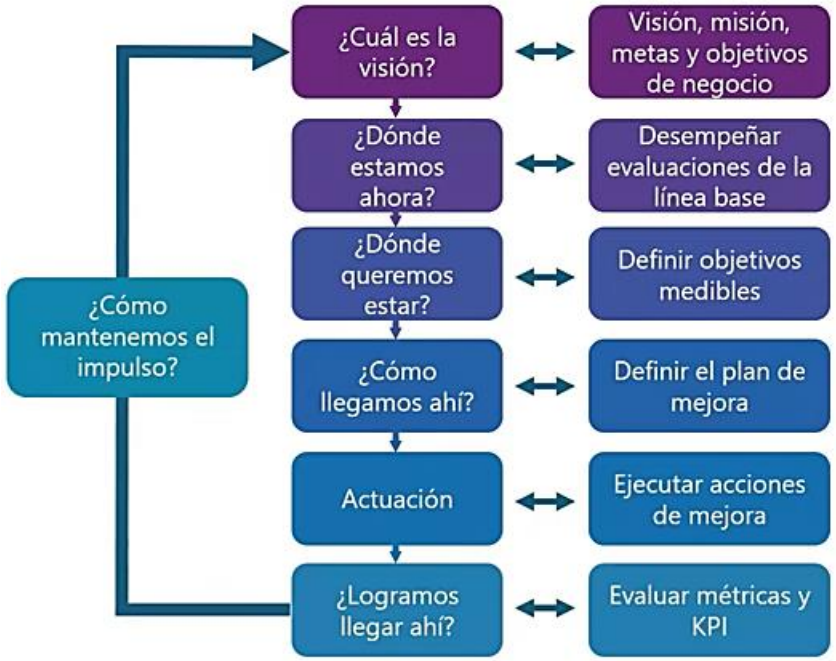
LA IDEA CENTRAL DE LA **MEJORA CONTINUA** EN EL CONTEXTO DE LA GESTIÓN DE SERVICIOS ES LA BÚSQUEDA CONSTANTE DE OPORTUNIDADES PARA MEJORAR LA EFICACIA Y LA EFICIENCIA DE LOS SERVICIOS **TI.**

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

MEJORA CONTINUA

Visión a alto nivel del modelo de mejora continua de ITIL



Guía a alto nivel para las mejoras:

- Aumenta el éxito de las iniciativas de ITSM;
- Se centra en el valor del cliente;
- Los esfuerzos de mejora vinculados a la visión;
- Enfoque iterativo;
- Elementos manejables con objetivos separados;
- Se consigue de manera gradual.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CERTIFICACIÓN ITIL

ACTUALMENTE EXISTEN DISTINTOS TIPOS DE CERTIFICACIONES ITIL DEPENDIENDO DEL NÚMERO DE CRÉDITOS Y DE LOS EXÁMENES SUPERADOS. ASÍ, PODEMOS ENCONTRAR PRINCIPALMENTE CUATRO TIPOS:

- **CERTIFICADO ITIL FOUNDATION**
- **CERTIFICADO ITIL MANAGING PROFESSIONAL**
- **CERTIFICADO STRATEGIC LEADER**
- **ITIL MÁSTER**

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CERTIFICACIÓN ITIL

- **CERTIFICADO ITIL FOUNDATION**

  ES EL NIVEL MÁS BÁSICO DE ITIL, YA QUE **PERMITE CONOCER LOS CONCEPTOS, TERMINOLOGÍA Y ESTRUCTURA UTILIZADOS EN ESTE SISTEMA DE GESTIÓN**. EL CERTIFICADO SE PUEDE OBTENER REALIZANDO UN CURSO DE 20 HORAS, QUE **PERMITE AL ALUMNO FAMILIARIZARSE CON LAS BUENAS PRÁCTICAS PARA LA GESTIÓN DE SERVICIOS EN LAS TECNOLOGÍAS DE LA INFORMACIÓN.** ESTE CERTIFICADO ES NECESARIO SI SE QUIERE ACCEDER A OTRO DE MÁS NIVEL.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CERTIFICACIÓN ITIL

- **CERTIFICADO ITIL MANAGING PROFESSIONAL**

  EN ESTE NIVEL **SE APRENDE A APLICAR ESAS BUENAS PRÁCTICAS DE GESTIÓN EN UNA EMPRESA,** YA QUE SE ADQUIEREN LAS CAPACIDADES Y HABILIDADES NECESARIAS PARA PONERLAS EN PRÁCTICA. SE DIRIGE A PROFESIONALES QUE TRABAJEN EN EQUIPOS DIGITALES Y DE TECNOLOGÍA, YA QUE LES **PROPORCIONA LOS CONOCIMIENTOS PRÁCTICOS PARA EJECUTAR LOS PROYECTOS Y SE CENTRA EN LA MEJORA CONTINUA DEL SERVICIO**. ESTE NIVEL CUENTA CON VARIOS MÓDULOS DE ITIL SPECIALIST: CREATE, DELIVER & SUPPORT, DRIVE STAKEHOLDER VALUE, HIGH VELOCITY IT Y DIRECT, PLAN Y STRATEGIST.

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CERTIFICACIÓN ITIL

- **CERTIFICADO STRATEGIC LEADER**

  ESTE NIVEL **PERMITE A LAS PERSONAS DEMOSTRAR UN CONOCIMIENTO SUPERIOR EN ITIL Y ENFOCADO A LA ESTRATEGIA DE NEGOCIO**. CUENTA CON DOS MÓDULOS, EL ITIL LEADER DIGITAL & IT STRATEGY Y ITIL SPECIALIST DIRECT, PLAN Y STRATEGIST.

- **ITIL MÁSTER**

  ES EL MÁXIMO NIVEL. PUEDE ALCANZARSE A TRAVÉS DE MÉRITOS PROFESIONALES DEMOSTRABLES, ES DECIR, **LO PUEDEN CONSEGUIR LAS PERSONAS QUE TENGAN EXPERIENCIA EN PROYECTOS REALES EN GESTIÓN DE SERVICIOS DE IT.**

3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

METODOLOGÍA ITIL

CERTIFICACIÓN ITIL

PARA OBTENER ESTAS CERTIFICACIONES HAY QUE SUPERAR UN EXAMEN QUE ACREDITE QUE SE TIENEN LAS CAPACIDADES NECESARIAS PARA OBTENER LA CERTIFICACIÓN A LA QUE SE ASPIRA. EXISTEN CURSOS QUE TE PREPARAN PARA ESTE EXAMEN Y CENTROS AUTORIZADOS PARA REALIZARLO.

LA CERTIFICACIÓN ITIL ES UNA FORMA DE QUE LAS PERSONAS ACREDITEN LAS BUENAS PRÁCTICAS QUE SON CAPACES DE LLEVAR A CABO EN LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN. ES IMPORTANTE RECORDAR QUE ESTE CERTIFICADO LO OBTIENE LA PERSONA, NO LA EMPRESA.

CONTENIDOS

1. INTRODUCCIÓN
2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN
4. **LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**
5. NORMATIVAS MÁS FRECUENTEMENTE UTILIZADAS PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

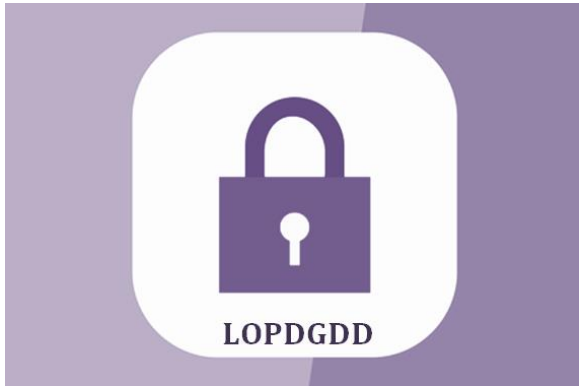
OBJETIVO, ESTRUCTURA Y ÁMBITO DE APLICACIÓN

LA PUBLICACIÓN DE LA **LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES** (**LOPDGDD**) PERSIGUE QUE LAS PERSONAS FÍSICAS PUEDAN EJERCER EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE SUS DATOS PERSONALES (ART. 18 CE).

NO OBSTANTE, EN ESPAÑA TAMBIÉN SE APLICA **EL REGLAMENTO (UE) 2016/679, DE 27 DE ABRIL (REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS O RGPD).**

Data Protection Reform

Reglamento UE 2016/679 del 27 abril de Protección de Datos Personales



4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

OBJETIVO, ESTRUCTURA Y ÁMBITO DE APLICACIÓN

ASÍ, LOS OBJETIVOS DE LA CITADA LEY SON:

- TRASPONER EL **REGLAMENTO (UE) 2016/679, DE 27 DE ABRIL (RGPD)** A LA NORMATIVA NACIONAL EN LO QUE RESPECTA A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN RELACIÓN AL TRATAMIENTO DE SUS DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS
- GARANTIZAR LOS DERECHOS DIGITALES A LA CIUDADANÍA ESPAÑOLA, EN RELACIÓN AL USO DE LA INFORMÁTICA PARA GARANTIZAR SU INTIMIDAD Y EL EJERCICIO DE SUS DERECHOS

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

OBJETIVO, ESTRUCTURA Y ÁMBITO DE APLICACIÓN

LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS TIENE UNA ESTRUCTURA COMPUESTA POR **97 ARTÍCULOS** RECOGIDOS EN **10 TÍTULOS**, ASÍ COMO NUMEROSAS DISPOSICIONES ENTRE ADICIONALES, TRANSITORIAS, DEROGATORIAS Y FINALES.

UN BREVE RESUMEN DE LO QUE REGULA CADA TÍTULO SE PRESENTA A CONTINUACIÓN:

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

OBJETIVO, ESTRUCTURA Y ÁMBITO DE APLICACIÓN

I. DISPOSICIONES GENERALES
II. PRINCIPIOS DE PROTECCIÓN DE DATOS
III. DERECHOS DE LAS PERSONAS FÍSICAS
IV. DISPOSICIONES SOBRE TRATAMIENTOS CONCRETOS
V. FIGURAS IMPLICADAS EN EL TRATAMIENTO DE DATOS Y MECANISMOS DE CERTIFICACIÓN
VI. TRANSFERENCIAS INTERNACIONALES DE DATOS
VII. AUTORIDADES DE PROTECCIÓN DE DATOS
VIII. PROCEDIMIENTOS APLICABLES EN LA VULNERACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS
IX. RÉGIMEN SANCIONADOR
X. DERECHOS DIGITALES DE LOS CIUDADANOS

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

OBJETIVO, ESTRUCTURA Y ÁMBITO DE APLICACIÓN

EL ÁMBITO DE APLICACIÓN DE LA **LOPDGDD** NO SE EXTIENDE A TODOS LOS ARTÍCULOS QUE LA INTEGRAN.

EN ELLA SE ESPECIFICA QUE SU ÁMBITO SOLO AFECTARÁ A LOS TÍTULOS I A IX, Y DE FORMA PARTICULAR, A LOS ARTÍCULOS 89 A 94 DEL TÍTULO X.

DE ESTA FORMA, TANTO EL ÁMBITO DE APLICACIÓN COMO EL DE NO APLICACIÓN DE LA LEY HACE REFERENCIA A LOS SIGUIENTES TRATAMIENTOS:

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

OBJETIVO, ESTRUCTURA Y ÁMBITO DE APLICACIÓN

APLICACIÓN

- TRATAMIENTO TOTAL O PARCIALMENTE AUTOMATIZADO DE DATOS PERSONALES.
- TRATAMIENTO NO AUTOMATIZADO DE DATOS PERSONALES INTEGRADOS O DESTINADOS A PERTENECER A UN FICHERO.

NO APLICACIÓN

- TRATAMIENTOS A LOS QUE NO SE LES APLICA EL RGPD.
- TRATAMIENTO DE DATOS DE PERSONAS FALLECIDAS, SALVO LO REGULADO POR EL ARTÍCULO 3 DE LA LEY.
- TRATAMIENTOS AMPARADOS POR LA NORMATIVA SOBRE PROTECCIÓN DE MATERIAS CLASIFICADAS.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPALES NOVEDADES DE LA LEY ORGÁNICA 3/2018

LA LOPDGDD AFECTA TANTO A PERSONAS FÍSICAS (AUTÓNOMOS) COMO JURÍDICAS (SOCIEDADES LIMITADAS, SOCIEDADES ANÓNIMAS, ETC.) ESTABLECIDAS O NO EN LA UNIÓN EUROPEA Y QUE TRATAN DATOS PERSONALES DE PERSONAS FÍSICAS SITUADAS EN LA UNIÓN.

ESTA LEY INTRODUCE **NOVEDADES** SOBRE ASPECTOS DE DIVERSA ÍNDOLE:

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPALES NOVEDADES DE LA LEY ORGÁNICA 3/2018

- TRATAMIENTO DE DATOS DE LAS PERSONAS FALLECIDAS
- FIJACIÓN DE LA EDAD DE LOS MENORES PARA DAR SU CONSENTIMIENTO EN 14 AÑOS
- LEGALIDAD EN EL TRATAMIENTO DE DETERMINADOS DATOS
  - DATOS DE CARÁCTER PENAL
  - DATOS DE CONTACTO, DE FUNCIÓN O DE PUESTO DE TRABAJO
  - DATOS INCLUIDOS EN UN SISTEMA DE INFORMACIÓN CREDITICIA
  - DATOS DERIVADOS DE OPERACIONES DE MODIFICACIÓN SOCIETARIA, APORTACIÓN O TRANSMISIÓN DE NEGOCIO
  - IMÁGENES OBTENIDAS POR SISTEMAS DE VIDEOVIGILANCIA
  - DATOS OBTENIDOS POR SISTEMAS DE INFORMACIÓN GENERAL O SECTORIAL
- SISTEMA DE INFORMACIÓN DE DENUNCIAS INTERNAS
- NUEVAS OBLIGACIONES DEL RESPONSABLE O ENCARGADO DEL TRATAMIENTO EN EL REGISTRO DE LAS ACTIVIDADES
- NUEVA OBLIGACIÓN DEL RESPONSABLE RESPECTO AL BLOQUEO DE DATOS
- RESPONSABILIDADES DEL DELEGADO DE PROTECCIÓN DE DATOS
- CONTENIDO, REGISTRO Y APROBACIÓN DE CÓDIGOS DE CONDUCTA
- REGULACIÓN DEL RÉGIMEN SANCIONADOR

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPALES NOVEDADES DE LA LEY ORGÁNICA 3/2018

LA MAYORÍA DE LAS ACTIVIDADES PROFESIONALES, ECONÓMICAS Y PRIVADAS QUE LAS PERSONAS REALIZAN **SE DESARROLLAN EN LA WEB**, LO QUE CONLLEVA UN RIESGO AÑADIDO. ES POR ESO QUE LOS ESTADOS ESTÁN PROMOVIENDO POLÍTICAS PARA QUE LOS CIUDADANOS PUEDAN EJERCER SUS DERECHOS FUNDAMENTALES EN LA REALIDAD DIGITAL.

EN ESTE SENTIDO, LA LEY ORGÁNICA 3/2018 RECOGE EN SU TÍTULO X LA REGULACIÓN DE DETERMINADOS DERECHOS APLICABLES A INTERNET. SON LOS DENOMINADOS **DERECHOS DIGITALES**.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPALES NOVEDADES DE LA LEY ORGÁNICA 3/2018

EN INTERNET

- DERECHO A LA NEUTRALIDAD.
- DERECHO DE ACCESO UNIVERSAL.
- DERECHO A LA SEGURIDAD DIGITAL.
- DERECHO A LA EDUCACIÓN DIGITAL.
- PROTECCIÓN DE LOS MENORES EN INTERNET.
- DERECHO DE RECTIFICACIÓN EN INTERNET.
- DERECHO A LA ACTUALIZACIÓN DE INFORMACIONES EN MEDIOS DE COMUNICACIÓN DIGITALES.
- PROTECCIÓN DE DATOS DE LOS MENORES EN INTERNET.
- DERECHO AL OLVIDO EN BÚSQUEDAS DE INTERNET.
- DERECHO AL OLVIDO EN SERVICIOS DE REDES SOCIALES Y SERVICIOS EQUIVALENTES.
- DERECHO DE PORTABILIDAD EN SERVICIOS DE REDES SOCIALES Y SERVICIOS EQUIVALENTES.
- DERECHO AL TESTAMENTO DIGITAL.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPALES NOVEDADES DE LA LEY ORGÁNICA 3/2018

EN EL ÁMBITO LABORAL

- DERECHO A LA INTIMIDAD Y USO DE DISPOSITIVOS DIGITALES.
- DERECHO A LA DESCONEXIÓN DIGITAL.
- DERECHO A LA INTIMIDAD FRENTE AL USO DE DISPOSITIVOS DE VIDEOVIGILANCIA Y DE GRABACIÓN DE SONIDOS EN EL LUGAR DE TRABAJO.
- DERECHO A LA INTIMIDAD ANTE LA UTILIZACIÓN DE SISTEMAS DE GEOLOCALIZACIÓN. DERECHOS DIGITALES EN LA NEGOCIACIÓN COLECTIVA.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

LA AUTORIDAD NACIONAL Y AUTONÓMICA DE PROTECCIÓN DE DATOS

LA AUTORIDAD DE CONTROL QUE SUPERVISA LA APLICACIÓN DE LA LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, Y DEL REGLAMENTO (UE) 2016/679, DE 27 DE ABRIL, ES LA **AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS** (**AEPD O AGENCIA**).

ADEMÁS, ES LA REPRESENTACIÓN DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS DE ESPAÑA ANTE EL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS.

LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS SE RELACIONA CON EL GOBIERNO A TRAVÉS DEL MINISTERIO DE JUSTICIA.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

LA AUTORIDAD NACIONAL Y AUTONÓMICA DE PROTECCIÓN DE DATOS

EL RGPD RECOGE QUE CADA ESTADO MIEMBRO DE LA UE PUEDE SUPERVISAR EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS CON UNA O VARIAS AUTORIDADES DE CONTROL.

EN ESTE SENTIDO, EN NUESTRO PAÍS EXISTEN, ADEMÁS DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, **DOS AUTORIDADES AUTONÓMICAS EN ESTA MATERIA:**

- **AGENCIA VASCA DE PROTECCIÓN DE DATOS**
- **AUTORIDAD CATALANA DE PROTECCIÓN DE DATOS**

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPIOS DE PROTECCIÓN DE DATOS DE LA LOPDGDD

LOS PRINCIPIOS DEL RGPD APLICABLES AL TRATAMIENTO SON *LICITUD, LEALTAD Y TRANSPARENCIA; LIMITACIÓN DE LA FINALIDAD; MINIMIZACIÓN DE LOS DATOS; EXACTITUD; LIMITACIÓN DEL PLAZO DE CONSERVACIÓN; INTEGRIDAD Y CONFIDENCIALIDAD, Y RESPONSABILIDAD PROACTIVA*. ADEMÁS DE ESTOS TAMBIÉN SE REGULA EL CONSENTIMIENTO, LA CATEGORÍA DE DATOS Y LOS TRATAMIENTOS QUE NO REQUIEREN IDENTIFICACIÓN.

SI SE COMPARAN ESTOS PRINCIPIOS CON LOS **REGULADOS POR LA LOPDGDD**, SE OBSERVA QUE NO TODOS ELLOS ESTÁN RELACIONADOS. DE ESTA MANERA, LOS QUE LA NORMATIVA NACIONAL HA DESARROLLADO BASÁNDOSE EN LA NORMATIVA EUROPEA SON:

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPIOS DE PROTECCIÓN DE DATOS DE LA LOPDGDD

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPIOS DE PROTECCIÓN DE DATOS DE LA LOPDGDD

EXACTITUD DE LOS DATOS

LOS DATOS RECABADOS POR EL RESPONSABLE DEL TRATAMIENTO **DEBEN SER EXACTOS A LOS FINES PARA LOS QUE SE TRATAN, Y ACTUALIZADOS, EN CASO NECESARIO.**

CUANDO LOS DATOS PERSONALES RECOGIDOS **SEAN INCORRECTOS RESPECTO A LOS FINES DEL TRATAMIENTO**, LA INEXACTITUD DE LOS MISMOS NO SERÁ ATRIBUIDA AL RESPONSABLE DEL TRATAMIENTO SI SE CUMPLEN LOS SIGUIENTES REQUISITOS:

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPIOS DE PROTECCIÓN DE DATOS DE LA LOPDGDD

EXACTITUD DE LOS DATOS

ACTUACIÓN DEL RESPONSABLE

EL RESPONSABLE DEL TRATAMIENTO DEBE HABER APLICADO LAS MEDIDAS ADECUADAS PARA ELIMINAR O RECTIFICAR, SIN DEMORA, LOS DATOS PERSONALES INEXACTOS.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPIOS DE PROTECCIÓN DE DATOS DE LA LOPDGDD

EXACTITUD DE LOS DATOS

FORMAS DE OBTENER LOS DATOS

LOS DATOS DEBEN HABER SIDO OBTENIDOS POR ALGUNA DE LAS SIGUIENTES FORMAS:

- DIRECTAMENTE DEL AFECTADO.
- DE UN MEDIADOR O INTERMEDIARIO QUE RECOJA EN NOMBRE PROPIO LA INFORMACIÓN PARA TRANSMITÍRSELA POSTERIORMENTE AL RESPONSABLE.
- DE OTRO RESPONSABLE, SIEMPRE Y CUANDO SEA PORQUE EL AFECTADO HA EJERCIDO SU DERECHO DE PORTABILIDAD.
- DE UN REGISTRO PÚBLICO.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPIOS DE PROTECCIÓN DE DATOS DE LA LOPDGDD

CONFIDENCIALIDAD DE LOS DATOS

EN EL TRATAMIENTO DE LOS DATOS PERSONALES, ESTÁN OBLIGADOS A CUMPLIR EL **DEBER DE CONFIDENCIALIDAD** LOS RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO, ADEMÁS DE TODOS AQUELLOS QUE INTERVENGAN EN EL MISMO.

ESTA OBLIGACIÓN SE MANTIENE, AUN CUANDO HAYA FINALIZADO LA RELACIÓN ENTRE EL RESPONSABLE O ENCARGADO DEL TRATAMIENTO Y EL INTERESADO.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPIOS DE PROTECCIÓN DE DATOS DE LA LOPDGDD

CONFIDENCIALIDAD DE LOS DATOS

PARA CUMPLIR LA OBLIGACIÓN DE CONFIDENCIALIDAD, SE DEBEN APLICAR **MEDIDAS TÉCNICAS Y ORGANIZATIVAS ADECUADAS QUE GARANTICEN LA SEGURIDAD DE LOS DATOS**, INCLUYENDO LA PROTECCIÓN CONTRA:

- **TRATAMIENTO NO AUTORIZADO**
- **TRATAMIENTO ILÍCITO**
- **PERDIDA**
- **DESTRUCCIÓN**
- **DAÑO ACCIDENTAL**

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPIOS DE PROTECCIÓN DE DATOS DE LA LOPDGDD

TRATAMIENTO DE DATOS POR EL RESPONSABLE PARA CUMPLIR UNA OBLIGACIÓN LEGAL O UNA TAREA DE CARÁCTER PÚBLICO

SEGÚN ESTE PRINCIPIO, SE CONSIDERA LÍCITO EL TRATAMIENTO DE DATOS PERSONALES REALIZADO POR EL RESPONSABLE CUANDO SEA NECESARIO PARA ALGUNOS DE LOS SIGUIENTES C**UMPLIMIENTOS**:

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPIOS DE PROTECCIÓN DE DATOS DE LA LOPDGDD

TRATAMIENTO DE DATOS POR EL RESPONSABLE PARA CUMPLIR UNA OBLIGACIÓN LEGAL O UNA TAREA DE CARÁCTER PÚBLICO

CUMPLIMIENTOS

DE UNA OBLIGACIÓN LEGAL DEL RESPONSABLE

ESTA OBLIGACIÓN DEBE ESTAR PREVISTA EN UNA NORMA EUROPEA O CON RANGO DE LEY, LA CUAL DETERMINARÁ LOS SIGUIENTES ASPECTOS:

- CONDICIONES GENERALES DEL TRATAMIENTO.
- TIPOS DE DATOS A TRATAR.
- CESIONES DE DATOS QUE PROCEDAN PARA CUMPLIR LA OBLIGACIÓN LEGAL.
- CONDICIONES ESPECIALES DE TRATAMIENTO BASADAS EN LA APLICACIÓN DE MEDIDAS ADICIONALES DE SEGURIDAD O EN OTRAS IMPUTADAS AL RESPONSABLE POR EL RGPD (CAPÍTULO IV).

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPIOS DE PROTECCIÓN DE DATOS DE LA LOPDGDD

TRATAMIENTO DE DATOS POR EL RESPONSABLE PARA CUMPLIR UNA OBLIGACIÓN LEGAL O UNA TAREA DE CARÁCTER PÚBLICO

CUMPLIMIENTOS

DE UNA LABOR CON CARÁCTER PÚBLICO

EN ESTE SUPUESTO, EL TRATAMIENTO SE DEBE CONSIDERAR NECESARIO PARA QUE EL RESPONSABLE PUEDA CUMPLIR CON UNA LABOR DE INTERÉS PÚBLICO O PARA QUE PUEDA EJERCER UN PODER PÚBLICO ASIGNADO.

EL TRATAMIENTO DEBE DERIVAR DE UNA COMPETENCIA ASIGNADA POR UNA NORMA CON RANGO DE LEY.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPIOS DE PROTECCIÓN DE DATOS DE LA LOPDGDD

CONSENTIMIENTO DEL INTERESADO. PARTICULARIDADES DE LOS MENORES DE EDAD

SEGÚN LA LOPDGDD, LOS DATOS PODRÁN SER OBJETO DE TRATAMIENTO SI LA PERSONA FÍSICA HUBIERA PRESTADO PREVIAMENTE SU **CONSENTIMIENTO EXPRESO** PARA ELLO.

EL RGPD RECOGE QUE, ADEMÁS DEL CONSENTIMIENTO, EXISTEN **OTRAS BASES JURÍDICAS** POR LAS QUE SE PERMITE EL TRATAMIENTO DE LOS DATOS PERSONALES. ENTRE OTRAS ESTÁN: **UNA RELACIÓN CONTRACTUAL** PREVIA QUE INCLUYA EL TRATAMIENTO, **UN INTERÉS LEGÍTIMO** QUE PREDOMINE SOBRE EL DERECHO DE LAS PERSONAS, ETC.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPIOS DE PROTECCIÓN DE DATOS DE LA LOPDGDD

CONSENTIMIENTO DEL INTERESADO. PARTICULARIDADES DE LOS MENORES DE EDAD

EL **CONSENTIMIENTO SE CARACTERIZA** POR LOS SIGUIENTES ASPECTOS, TANTO A NIVEL GENERAL COMO PARA LOS MENORES DE EDAD:

CARACTERÍSTICAS GENERALES

- CUANDO EL TRATAMIENTO DE LOS DATOS TENGA POR OBJETO VARIOS FINES DE DISTINTA NATURALEZA, DEBE CONSTAR ESPECÍFICAMENTE QUE EL INTERESADO DA SU CONSENTIMIENTO PARA TODOS ELLOS.
- EL CONSENTIMIENTO SE PUEDE PRESTAR MEDIANTE UNA DECLARACIÓN (VERBAL, POR ESCRITO U OTRO MEDIO) O A TRAVÉS DE UNA ACCIÓN AFIRMATIVA.
- SI EL CONSENTIMIENTO SE PRESTA MEDIANTE UNA DECLARACIÓN ESCRITA JUNTO A OTROS DATOS, ESTE DEBE DISTINGUIRSE CLARAMENTE DEL RESTO, DEBE ESTAR ESCRITO DE FORMA INTELIGIBLE, SER DE FÁCIL ACCESO Y TENER UN LENGUAJE CLARO Y SENCILLO.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPIOS DE PROTECCIÓN DE DATOS DE LA LOPDGDD

CONSENTIMIENTO DEL INTERESADO. PARTICULARIDADES DE LOS MENORES DE EDAD

CARACTERÍSTICAS GENERALES

- LA EJECUCIÓN DE UN CONTRATO NO PUEDE DEPENDER DEL CONSENTIMIENTO DEL INTERESADO AL TRATAMIENTO DE SUS DATOS, CUANDO LOS FINES SEAN DISTINTOS A LOS DEL CONTRATO.
- CUANDO EXISTA OTRA BASE JURÍDICA QUE LEGITIME EL TRATAMIENTO DE LOS DATOS, NO SERÁ NECESARIO EL CONSENTIMIENTO POR PARTE DEL INTERESADO.
- EL TRATAMIENTO DE LOS DATOS PERSONALES DE LOS CIUDADANOS, QUE TENGA POR OBJETO LA VERIFICACIÓN DE LOS MISMOS POR PARTE DE LAS ADMINISTRACIONES PÚBLICAS, SE REALIZARÁ SIN RECABAR CONSENTIMIENTO ALGUNO. SIN EMBARGO, SÍ SERÁ NECESARIO CUANDO DICHOS ORGANISMOS DEBAN COMUNICAR LOS DATOS A TERCEROS (CARÁCTER PRIVADO).

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPIOS DE PROTECCIÓN DE DATOS DE LA LOPDGDD

CONSENTIMIENTO DEL INTERESADO. PARTICULARIDADES DE LOS MENORES DE EDAD

CARACTERÍSTICAS GENERALES

- NO SERÁ NECESARIO EL CONSENTIMIENTO DEL CIUDADANO CUANDO SE TRATEN LOS DATOS POR ORGANISMOS PÚBLICOS EN CUMPLIMIENTO DE UNA MISIÓN DE INTERÉS PÚBLICO O EN EL EJERCICIO DE PODERES PÚBLICOS.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

PRINCIPIOS DE PROTECCIÓN DE DATOS DE LA LOPDGDD

CONSENTIMIENTO DEL INTERESADO. PARTICULARIDADES DE LOS MENORES DE EDAD

CARACTERÍSTICAS DE LOS MENORES DE EDAD

- CUANDO EXISTA EL CONSENTIMIENTO DEL MENOR DE EDAD Y ESTE TENGA COMO MÍNIMO 14 AÑOS. SALVO QUE POR LEY SE DETERMINE LA ASISTENCIA DEL TITULAR DE LA PATRIA POTESTAD O TUTELA AL ACTO POR EL CUAL EL MENOR DEBA PRESTAR CONSENTIMIENTO EN EL TRATAMIENTO DE SUS DATOS.
- CUANDO EL MENOR DE EDAD TENGA UNA EDAD INFERIOR A 14 AÑOS Y EXISTA EL CONSENTIMIENTO DEL TITULAR DE LA PATRIA POTESTAD O TUTELA, CON EL ALCANCE QUE ESTOS DETERMINEN.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

CATEGORÍAS DE LOS DATOS

LA INFORMACIÓN QUE SE RECOGE DE UNA PERSONA FÍSICA PUEDE SER DE DIFERENTES TIPOS, LO QUE IMPLICA QUE LAS MEDIDAS DE SEGURIDAD SERÁN DISTINTAS DEPENDIENDO DE LA CATEGORÍA DE LOS DATOS QUE SE TRATEN. SEGÚN LA LEY ORGÁNICA, Y DE FORMA COMPLEMENTARIA EL RGPD, EXISTEN LAS SIGUIENTES **CATEGORÍAS DE DATOS**:

- **BÁSICOS**
- **ESPECIALES**
- **DE NATURALEZA PENAL**

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

CATEGORÍAS DE LOS DATOS

BÁSICOS

SE CONSIDERAN COMO DATOS BÁSICOS TODOS AQUELLOS QUE PUEDAN IDENTIFICAR A UNA PERSONA FÍSICA, QUE NO ESTÉN INCLUIDOS DENTRO DE UNA CATEGORÍA ESPECIAL Y QUE NO TENGAN NATURALEZA PENAL.

ENTRE ELLOS ESTÁN: NOMBRE Y APELLIDOS, NIF, ESTADO CIVIL, AFICIONES, PUESTO DE TRABAJO, CUENTA CORRIENTE, ETC.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

CATEGORÍAS DE LOS DATOS

BÁSICOS

EL TRATAMIENTO DE ESTA CATEGORÍA DE DATOS SE BASA EN LO QUE SE ENTIENDE POR DATOS DE CARÁCTER PERSONAL, QUE ES TODA LA INFORMACIÓN RELATIVA A UNA PERSONA FÍSICA IDENTIFICADA O IDENTIFICABLE (DATOS CONCERNIENTES AL INTERESADO).

LAS MEDIDAS A APLICAR PARA GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN TRATADA VAN A DEPENDER DE CADA ORGANIZACIÓN Y DEL NIVEL DE RIESGO QUE ESTA DISPONGA.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

CATEGORÍAS DE LOS DATOS

ESPECIALES

SE INCLUYEN EN ESTA CATEGORÍA LOS DATOS DEL ORIGEN ÉTNICO O RACIAL; IDEOLOGÍA Y RELIGIÓN; AFILIACIÓN SINDICAL; RELATIVOS A LA SALUD, Y LOS RELACIONADOS CON LA ORIENTACIÓN SEXUAL DE LA PERSONA.

CON CARÁCTER GENERAL, EL TRATAMIENTO DE ESTA CATEGORÍA ESTÁ PROHIBIDO, INCLUSO CUANDO EXISTA EL CONSENTIMIENTO EXPRESO DEL INTERESADO. SIN EMBARGO, ESTA PROHIBICIÓN NO SE APLICARÁ SI SE CUMPLE UNA DE LAS **CIRCUNSTANCIAS** ESTABLECIDAS EN EL ARTÍCULO 9.2 DEL RGPD.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

CATEGORÍAS DE LOS DATOS

ESPECIALES

SE PODRÁ REALIZAR EL TRATAMIENTO DE LOS DATOS DE ESTA CATEGORÍA CUANDO:

- EXISTA UN CONSENTIMIENTO EXPLÍCITO PARA FINES ESPECÍFICOS.
- SEA NECESARIO PARA CUMPLIR OBLIGACIONES Y EJERCER DERECHOS POR PARTE DEL RESPONSABLE Y DEL INTERESADO.
- LO REALICE UNA FUNDACIÓN, ASOCIACIÓN U ORGANISMO SIN ÁNIMO DE LUCRO, A SUS MIEMBROS Y CON UN FIN PRECISO.
- SEAN MANIFIESTAMENTE PÚBLICOS.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

CATEGORÍAS DE LOS DATOS

ESPECIALES

- SE DEBAN PROTEGER LOS INTERESES DEL AFECTADO SI NO ESTÁ CAPACITADO PARA PRESTAR CONSENTIMIENTO. SEA NECESARIO PARA LA TRAMITACIÓN DE RECLAMACIONES, PARA FINES DE ARCHIVO, DE INVESTIGACIÓN CIENTÍFICA, HISTÓRICA O ESTADÍSTICA.
- EL TRATAMIENTO DE DATOS RELACIONADOS CON LA SALUD. SE REALICEN POR CAUSAS MÉDICAS, DE SALUD PÚBLICA O DE INVESTIGACIÓN CIENTÍFICA O ESTADÍSTICA; LO ESTABLEZCAN LOS SISTEMAS O SERVICIOS DE ASISTENCIA SANITARIA O SOCIAL (PÚBLICA O PRIVADA), O POR LA EJECUCIÓN DE UN CONTRATO DE SEGURO DEL INTERESADO.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

CATEGORÍAS DE LOS DATOS

DE NATURALEZA PENAL

EN ESTA CATEGORÍA SE INCLUYEN DATOS RELACIONADOS CON CONDENAS E INFRACCIONES PENALES DEL INTERESADO, Y PROCEDIMIENTOS Y MEDIDAS CAUTELARES Y DE SEGURIDAD CONEXAS. EL TRATAMIENTO DE ESTA CATEGORÍA DE DATOS ÚNICAMENTE PUEDE REALIZARSE EN LOS SIGUIENTES CASOS:

- CUANDO ASÍ LO REGULE UNA NORMA EUROPEA, LA LOPDGDD U OTRA NORMA CON RANGO DE LEY.
- SOLO PODRÁ LLEVARSE UN REGISTRO COMPLETO DE CONDENAS PENALES CUANDO SE REALICE BAJO EL CONTROL DE LAS AUTORIDADES PÚBLICAS.
- CUANDO LO REALICEN ABOGADOS O PROCURADORES EN EL EJERCICIO DE SUS FUNCIONES.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

EL RESPONSABLE Y EL ENCARGADO DEL TRATAMIENTO

EL RESPONSABLE Y EL ENCARGADO DEL TRATAMIENTO SE IDENTIFICAN COMO TODA **PERSONA FÍSICA O JURÍDICA, AUTORIDAD PÚBLICA, SERVICIO U OTROS ORGANISMOS**, CUYAS COMPETENCIAS PROPIAS SON:

- **RESPONSABLE DEL TRATAMIENTO.** DETERMINAR LOS FINES Y MEDIOS DEL TRATAMIENTO, SOLO O JUNTO CON OTROS
- **ENCARGADO DEL TRATAMIENTO.** TRATAR DATOS PERSONALES POR CUENTA DEL RESPONSABLE DEL TRATAMIENTO

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

EL RESPONSABLE Y EL ENCARGADO DEL TRATAMIENTO

CON CARÁCTER GENERAL, LAS FIGURAS DEL RESPONSABLE Y DEL ENCARGADO SON DISTINTAS, POR ELLO ES ADECUADO SABER DISTINGUIRLOS.

LOS RESPONSABLES Y ENCARGADOS TIENEN LA **OBLIGACIÓN DE APLICAR MEDIDAS TÉCNICAS Y ORGANIZATIVAS ADECUADAS** PARA GARANTIZAR Y DEMOSTRAR QUE EL TRATAMIENTO ESTÁ AJUSTADO AL **RGPD** Y A LA **LOPDGDD**, Y QUE SE CUMPLE CON EL **PRINCIPIO DE LA PROTECCIÓN DE DATOS** DESDE EL DISEÑO Y POR DEFECTO. CONCRETAMENTE, VALORARÁN LA REALIZACIÓN DE LA **EVALUACIÓN DE IMPACTO** Y LA **CONSULTA PREVIA** AL TRATAMIENTO.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

EL DELEGADO DE PROTECCIÓN DE DATOS

EL DELEGADO DE PROTECCIÓN DE DATOS (DPD) ES **EL INTERLOCUTOR DEL RESPONSABLE O ENCARGADO DEL TRATAMIENTO ANTE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) Y LAS AUTORIDADES AUTONÓMICAS**.

ADEMÁS, TIENE POTESTAD PARA INSPECCIONAR LOS PROCEDIMIENTOS REALIZADOS AL AMPARO DE LA LEY Y PARA EMITIR LAS RECOMENDACIONES OPORTUNAS.

LA DESIGNACIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS CORRESPONDE AL RESPONSABLE Y AL ENCARGADO DEL TRATAMIENTO, TENIENDO LA CONSIDERACIÓN DE **FIGURA VOLUNTARIA**.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

EL DELEGADO DE PROTECCIÓN DE DATOS

CUALIFICACIÓN DEL DPD

SEGÚN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS, EL **DPD** PARA DESEMPEÑAR SUS FUNCIONES (ART. 39) DEBE TENER:

CUALIDADES PROFESIONALES RELACIONADAS CON CONOCIMIENTOS EN DERECHO. PRÁCTICA EN EL ÁMBITO DE LA PROTECCIÓN DE DATOS.

EN ESTE SENTIDO, LA LOPDGDD RECOGE QUE, PARA DEMOSTRAR EL CUMPLIMIENTO DE DICHOS REQUISITOS, SE PUEDEN UTILIZAR, ENTRE OTROS, MECANISMOS VOLUNTARIOS DE ACREDITACIÓN, LOS CUALES TENDRÁN EN CUENTA LA TITULACIÓN UNIVERSITARIA CORRESPONDIENTE Y LA PRÁCTICA REQUERIDA EN ESTA MATERIA.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

EL DELEGADO DE PROTECCIÓN DE DATOS

CARACTERÍSTICAS DEL DPD

LAS CARACTERÍSTICAS DE ESTA FIGURA, CON CARÁCTER GENERAL, SON:

- PUEDE SER TANTO UNA PERSONA FÍSICA (EMPLEADO EN PLANTILLA, AUTÓNOMO) COMO UNA PERSONA JURÍDICA (EMPRESA).
- PUEDE EJERCER SUS FUNCIONES A TIEMPO COMPLETO O PARCIAL, SIENDO EL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO QUIENES LO DECIDIRÁN EN FUNCIÓN DEL VOLUMEN DE TRATAMIENTOS, DE LA CATEGORÍA ESPECIAL DE LOS DATOS O DE LOS RIESGOS.
- SI ES INTEGRANTE DE LA PLANTILLA DE LA EMPRESA, NO PUEDE SER TRASLADADO NI SANCIONADO POR EL RESPONSABLE O ENCARGADO DEL TRATAMIENTO POR LA REALIZACIÓN DE SUS FUNCIONES, SALVO QUE COMETA UNA FALTA GRAVE.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

EL DELEGADO DE PROTECCIÓN DE DATOS

CARACTERÍSTICAS DEL DPD

- SE DEBE GARANTIZAR LA INDEPENDENCIA DEL DPD, EVITANDO CONFLICTOS DE INTERESES ENTRE LOS MIEMBROS DE LA EMPRESA.
- EL RESPONSABLE O EL ENCARGADO DEL TRATAMIENTO, AL AMPARO DEL DEBER DE CONFIDENCIALIDAD, NO PUEDEN OPONERSE A QUE EL DPD ACCEDA A LOS DATOS PERSONALES O A LOS PROCESOS DE TRATAMIENTO.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

DERECHOS DE LAS PERSONAS EN LA PROTECCIÓN DE SUS DATOS

TAL Y COMO SE HA INDICADO, EL REGLAMENTO (UE) 2016/679 RECOGE EN SU ARTICULADO UN GRUPO DE **DERECHOS RELACIONADOS CON EL TRATAMIENTO DE LOS DATOS PERSONALES DE LAS PERSONAS FÍSICAS**, SON LOS SIGUIENTES:

- **DERECHO DE ACCESO**
- **DERECHOS DE RECTIFICACIÓN**
- **DERECHO DE SUPRESIÓN O DERECHO AL OLVIDO**
- **DERECHO A LA LIMITACIÓN DEL TRATAMIENTO**
- **DERECHO A LA PORTABILIDAD DE LOS DATOS**
- **DERECHO DE OPOSICIÓN Y A LAS DECISIONES INDIVIDUALES AUTOMATIZADAS**

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

DERECHOS DE LAS PERSONAS EN LA PROTECCIÓN DE SUS DATOS

DERECHO DE ACCESO

LA LOPDGDD ESTABLECE QUE EL INTERESADO PUEDE EJERCER EL DERECHO DE ACCESO ATENDIENDO A LO QUE RECOGE EL RGPD SOBRE ÉL.

DE ESTA MANERA, ESTE DERECHO **PERMITE A LOS INTERESADOS CONTROLAR EL USO, CONOCER Y OBTENER INFORMACIÓN SOBRE EL TRATAMIENTO**, REALIZADO POR UNA EMPRESA PÚBLICA O PRIVADA, **DE SUS DATOS PERSONALES**.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

DERECHOS DE LAS PERSONAS EN LA PROTECCIÓN DE SUS DATOS

DERECHO DE RECTIFICACIÓN

EL INTERESADO PUEDE EJERCER EL DERECHO DE RECTIFICACIÓN TENIENDO EN CUENTA LOS FINES DEL TRATAMIENTO. DEBERÁ SEGUIR LO REGULADO TANTO EN EL RGPD COMO EN LA LOPDGDD:

RGPD

EL INTERESADO TIENE DERECHO A OBTENER, POR PARTE DEL RESPONSABLE DEL TRATAMIENTO, LA RECTIFICACIÓN DE SUS DATOS PERSONALES CUANDO RESULTEN INEXACTOS E INCOMPLETOS, SIN EXISTIR DILACIÓN INDEBIDA EN ELLO.

LOPDGDD

EN LA SOLICITUD DEL INTERESADO PARA EJERCER EL DERECHO CONSTARÁN LOS DATOS A LOS QUE SE REFIERE Y LA CORRECCIÓN A REALIZAR; IGUALMENTE SE PODRÁ ADJUNTAR LA DOCUMENTACIÓN QUE JUSTIFIQUE LA INEXACTITUD O EL CARÁCTER INCOMPLETO DE LOS DATOS.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

DERECHOS DE LAS PERSONAS EN LA PROTECCIÓN DE SUS DATOS

DERECHO DE SUPRESIÓN O DERECHO AL OLVIDO

EL **DERECHO DE SUPRESIÓN O DERECHO AL OLVIDO** DEBE SER EJERCIDO POR EL INTERESADO SIGUIENDO LAS PAUTAS DEL RGPD Y DE LA LOPDGDD.

SEGÚN EL REGLAMENTO, ESTE DERECHO TIENE COMO FINALIDAD **IMPEDIR LA DIFUSIÓN DE INFORMACIÓN PERSONAL A TRAVÉS DE INTERNET** CUANDO SU PUBLICACIÓN NO CUMPLE LOS REQUISITOS DE ADECUACIÓN Y PERTINENCIA PREVISTOS EN LA NORMATIVA, SEA OBSOLETA, INCOMPLETA, FALSA O IRRELEVANTE Y NO SEA DE INTERÉS PÚBLICO, ENTRE OTROS MOTIVOS.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

DERECHOS DE LAS PERSONAS EN LA PROTECCIÓN DE SUS DATOS

DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

ESTE DERECHO HA SIDO DESARROLLADO POR EL RGPD, REGULANDO ÚNICAMENTE LA LOPDGDD UNA OBLIGACIÓN DEL RESPONSABLE.

EL **RGPD** ESTABLECE QUE EL INTERESADO DISPONDRÁ DE AUTORIDAD PARA SOLICITAR DEL RESPONSABLE LA **LIMITACIÓN EN EL TRATAMIENTO DE SUS DATOS** SIEMPRE Y CUANDO SE CUMPLA ALGUNAS DE LAS SIGUIENTES CONDICIONES:

- **INEXACTITUD**
- **ILICITUD**
- **RECLAMACIONES**
- **OPOSICIÓN**

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

DERECHOS DE LAS PERSONAS EN LA PROTECCIÓN DE SUS DATOS

DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

INEXACTITUD

EL INTERESADO IMPUGNE LA EXACTITUD DE LOS DATOS PERSONALES, DURANTE UN PLAZO QUE PERMITA AL RESPONSABLE LA VERIFICACIÓN DE LOS MISMOS.

ILICITUD

EL TRATAMIENTO SEA ILÍCITO Y EL INTERESADO SE OPONGA A LA SUPRESIÓN DE LOS DATOS PERSONALES Y SOLICITE EN SU LUGAR LA LIMITACIÓN DE SU USO.

RECLAMACIONES

EL RESPONSABLE YA NO NECESITE LOS DATOS PARA LOS FINES DEL TRATAMIENTO, PERO EL INTERESADO SÍ, PARA LA FORMULACIÓN, EL EJERCICIO O LA DEFENSA DE RECLAMACIONES.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

DERECHOS DE LAS PERSONAS EN LA PROTECCIÓN DE SUS DATOS

DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

OPOSICIÓN

EL INTERESADO SE HAYA OPUESTO AL TRATAMIENTO MIENTRAS SE VERIFICA SI LOS MOTIVOS LEGÍTIMOS DEL RESPONSABLE PREVALECEN SOBRE LOS SUYOS.

CUANDO SE PRODUZCA EL **LEVANTAMIENTO DE LA LIMITACIÓN EN EL TRATAMIENTO DE LOS DATOS**, EL INTERESADO TIENE DERECHO A SER INFORMADO.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

DERECHOS DE LAS PERSONAS EN LA PROTECCIÓN DE SUS DATOS

DERECHO A LA PORTABILIDAD DE LOS DATOS

LA LOPDGDD SOLO DETERMINA QUE SE DEBE EJERCER ESTE DERECHO CONFORME A LO DICTADO POR EL RGPD, EN EL CUAL SE ESTABLECE QUE ESTE DERECHO POSIBILITA AL INTERESADO LA **TRANSMISIÓN DE DATOS PERSONALES DE UN RESPONSABLE A OTRO**. SUS CARACTERÍSTICAS SON:

1. EL INTERESADO TENDRÁ DERECHO A RECIBIR LOS DATOS FACILITADOS A UN RESPONSABLE Y A TRANSMITIRLOS A OTRO.
2. LOS DATOS DEBEN SER ENTREGADOS AL INTERESADO EN UN FORMATO ESTRUCTURADO, DE USO COMÚN Y LECTURA MECÁNICA.
3. EL RESPONSABLE INICIAL NO PUEDE IMPEDIR LA TRANSMISIÓN DE LOS DATOS, SIEMPRE QUE EL TRATAMIENTO ESTUVIERA BASADO EN EL CONSENTIMIENTO, EN UN CONTRATO O SE REALICE POR MEDIOS AUTOMATIZADOS.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

DERECHOS DE LAS PERSONAS EN LA PROTECCIÓN DE SUS DATOS

DERECHO A LA PORTABILIDAD DE LOS DATOS

4. EL EJERCICIO DE ESTE DERECHO SE ENTENDERÁ SIN PERJUICIO DEL EJERCICIO DEL DERECHO AL OLVIDO.
5. ESTE DERECHO NO SE LIMITA SOLO A LOS DATOS PROPORCIONADOS DE FORMA DIRECTA POR EL INTERESADO, SINO QUE ABARCA TAMBIÉN LOS GENERADOS EN LA ACTIVIDAD.
6. NO SE APLICARÁ AL TRATAMIENTO NECESARIO PARA CUMPLIR UNA TAREA REALIZADA EN INTERÉS PÚBLICO O EN EL EJERCICIO DE PODERES PÚBLICOS DEL RESPONSABLE.
7. EL EJERCICIO DE ESTE DERECHO NO PUEDE AFECTAR NEGATIVAMENTE A LOS DERECHOS Y LIBERTADES DE OTROS DERECHOS.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

DERECHOS DE LAS PERSONAS EN LA PROTECCIÓN DE SUS DATOS

DERECHO DE OPOSICIÓN Y A LAS DECISIONES INDIVIDUALES AUTOMATIZADAS

A TRAVÉS DEL DERECHO DE OPOSICIÓN, CONTEMPLADO EN EL RGPD Y EN LA LOPDGDD, EL INTERESADO PUEDE **OPONERSE AL TRATAMIENTO DE SUS DATOS PERSONALES** EN CUALQUIER MOMENTO, POR CAUSAS RELACIONADAS CON SU SITUACIÓN PARTICULAR Y EN ALGUNAS DE LAS SIGUIENTES **SITUACIONES**:

- SE REALICE CON FINES DE MERCADOTECNIA DIRECTA.
- SE BASE EN LA ELABORACIÓN DE PERFILES.
- SEA DE INTERÉS LEGÍTIMO DEL RESPONSABLE O TERCEROS, SIEMPRE QUE NO
- PREVALEZCAN LOS INTERESES O LOS DERECHOS Y LIBERTADES DEL INTERESADO.
- SE BASE EN INVESTIGACIÓN HISTÓRICA, ESTADÍSTICA O CIENTÍFICA, SALVO QUE EL TRATAMIENTO SEA NECESARIO POR MOTIVOS DE INTERÉS PÚBLICO.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

LOS DERECHOS EN LA ERA DIGITAL

LOS **DERECHOS Y LIBERTADES** CONFIRMADOS POR LA CONSTITUCIÓN, ASÍ COMO POR LOS TRATADOS INTERNACIONALES EN LOS QUE NUESTRO PAÍS TIENE PARTICIPACIÓN, **SON APLICABLES EN INTERNET**.

LA LOPDGDD INTRODUCE COMO NOVEDAD, EN EL ÁMBITO DE LA PROTECCIÓN DE DATOS, EL **TÍTULO X. GARANTÍA DE LOS DERECHOS DIGITALES**.

EL CONJUNTO DE DERECHOS QUE REGULA ESTE TÍTULO SE PUEDE AGRUPAR DEPENDIENDO DE VARIOS FACTORES:

- **DERECHOS GENERALES DE LAS PERSONAS EN INTERNET**
- **DERECHOS EN EL ÁMBITO LABORAL**
- **DERECHOS DE LOS MENORES**

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

LOS DERECHOS EN LA ERA DIGITAL

DERECHOS GENERALES DE LAS PERSONAS EN INTERNET

- DERECHO A LA NEUTRALIDAD EN INTERNET.
- DERECHO DE ACCESO UNIVERSAL A INTERNET.
- DERECHO A LA SEGURIDAD DIGITAL.
- DERECHO DE RECTIFICACIÓN EN INTERNET.
- DERECHO A LA ACTUALIZACIÓN DE INFORMACIONES EN MEDIOS DE COMUNICACIÓN DIGITALES.
- DERECHO AL OLVIDO EN BÚSQUEDAS DE INTERNET.
- DERECHO AL OLVIDO EN SERVICIOS DE REDES SOCIALES Y SERVICIOS EQUIVALENTES.
- DERECHO DE PORTABILIDAD EN SERVICIOS DE REDES SOCIALES Y SERVICIOS EQUIVALENTES.
- DERECHO AL TESTAMENTO DIGITAL.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

LOS DERECHOS EN LA ERA DIGITAL

DERECHOS EN EL ÁMBITO LABORAL

- DERECHO A LA INTIMIDAD Y USO DE DISPOSITIVOS DIGITALES.
- DERECHO A LA DESCONEXIÓN DIGITAL.
- DERECHO A LA INTIMIDAD FRENTE AL USO DE DISPOSITIVOS DE VIDEOVIGILANCIA Y DE GRABACIÓN
- DE SONIDOS EN EL LUGAR DE TRABAJO.
- DERECHO A LA INTIMIDAD ANTE LA UTILIZACIÓN DE SISTEMAS DE GEOLOCALIZACIÓN.
- DERECHOS DIGITALES EN LA NEGOCIACIÓN COLECTIVA.

4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

LOS DERECHOS EN LA ERA DIGITAL

DERECHOS DE LOS MENORES

- DERECHO A LA EDUCACIÓN DIGITAL.
- PROTECCIÓN DE LOS MENORES EN INTERNET.
- PROTECCIÓN DE DATOS DE LOS MENORES EN INTERNET.

CONTENIDOS

1. INTRODUCCIÓN
2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN
4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
5. **NORMATIVAS MÁS FRECUENTEMENTE UTILIZADAS PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA**

5. NORMATIVAS MÁS FRECUENTEMENTE UTILIZADAS PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA

EN LA ACTUALIDAD LA INFORMACIÓN SE ALMACENA EN **LOS EQUIPOS INFORMÁTICOS**, EN LOS DIFERENTES **SOPORTES DE ALMACENAMIENTO** Y EN **LAS REDES DE DATOS** DONDE SE GUARDA LA GRAN MAYORÍA DE ELLA, CONSTITUYENDO ASÍ EL CONJUNTO DE ESTOS TRES CONTENEDORES DE INFORMACIÓN LOS LLAMADOS **SISTEMAS DE INFORMACIÓN**.

LA INFORMACIÓN ES EL PRINCIPAL ACTIVO DE LAS ORGANIZACIONES Y, POR LO TANTO, LOS LUGARES EN LOS QUE ELLA RESIDE HAN DE ESTAR PROTEGIDOS CONVENIENTEMENTE, TANTO DE POSIBLES ACCESOS A ELLA NO AUTORIZADOS COMO DEL RIESGO A QUE LA INFORMACIÓN SE PIERDA DEBIDO A ALGÚN FALLO EN LOS SISTEMAS DE INFORMACIÓN OCASIONADOS POR CIRCUNSTANCIAS AJENAS A LA VOLUNTAD HUMANA, COMO PUEDEN SER DISTINTOS FENÓMENOS NATURALES.

5. NORMATIVAS MÁS FRECUENTEMENTE UTILIZADAS PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA

PODEMOS DISTINGUIR LOS DOS TIPOS DE RIESGOS A LOS QUE ESTÁN EXPUESTOS NUESTROS SISTEMAS DE INFORMACIÓN Y DE CUYA MINIMIZACIÓN SE ENCARGA LA SEGURIDAD INFORMÁTICA:

- **RIESGOS LÓGICOS**
- **RIESGOS FÍSICOS**

5. NORMATIVAS MÁS FRECUENTEMENTE UTILIZADAS PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA

RIESGOS LÓGICOS

SON LOS RIESGOS ASOCIADOS A LA TECNOLOGÍA DE LOS PROPIOS SISTEMAS DE INFORMACIÓN Y QUE AFECTAN DIRECTAMENTE A SU SOFTWARE, SON RIESGOS DIFÍCILES DE DETECTAR, RAZÓN DE MÁS PARA CONSIDERARLOS MUY PELIGROSOS. LAS ALTERACIONES QUE PROVOCAN EN EL FUNCIONAMIENTO NORMAL DEL SISTEMA PUEDEN LLEGAR A OCASIONAR DAÑOS IRREPARABLES EN EL SISTEMA SON RIESGOS DE ESTE TIPO LOS CÓDIGOS MALICIOSOS, EL SPAM, LA PIRATERÍA (HACKERS), LA FUGA DE INFORMACIÓN O LA INGENIERÍA SOCIAL. LOS PROBLEMAS OCASIONADOS POR ESTE TIPO DE RIESGOS PUEDEN DAÑAR SERIAMENTE LA IMAGEN DE NUESTRA ORGANIZACIÓN.

5. NORMATIVAS MÁS FRECUENTEMENTE UTILIZADAS PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA

RIESGOS FÍSICOS

SE ENGLOBAN EN ESTE PUNTO AQUELLOS RIESGOS, QUE DE UNA U OTRA FORMA PUEDEN AFECTAR A LA CONTINUIDAD DE LOS PROCESOS DE NEGOCIO DE LA ORGANIZACIÓN POR AFECTAR A LA DISPONIBILIDAD DE LA INFORMACIÓN, SU PRINCIPAL ACTIVO. SON CONSIDERADOS RIESGOS FÍSICOS PARA LOS SISTEMAS INFORMÁTICOS LOS FENÓMENOS NATURALES COMO INCENDIOS, INUNDACIONES, TERREMOTOS, ETC., LOS ACTOS VANDÁLICOS O LOS PROBLEMAS ELÉCTRICOS Y ELECTROMAGNÉTICOS.

5. NORMATIVAS MÁS FRECUENTEMENTE UTILIZADAS PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA

EN LA ACTUALIDAD ES TAL EL NIVEL DE RIESGO, QUE **LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN SE DEBE CONSIDERAR ALGO IMPRESCINDIBLE**.

DEBEMOS DE CONOCER LAS AMENAZAS A LAS QUE ESTAMOS SOMETIDOS Y DEBEMOS SABER CÓMO AFRONTARLAS ADECUADAMENTE Y LAS HERRAMIENTAS Y NORMATIVA QUE PARA ELLO TENEMOS DISPONIBLE.

DEBEMOS DE TENER ESTABLECIDOS PROCEDIMIENTOS ADECUADOS PARA CONTRARRESTARLAS E IMPLEMENTAR TODOS LOS CONTROLES DE SEGURIDAD QUE SEAN NECESARIOS.

DICHOS CONTROLES SE BASAN TANTO EN EVALUAR LOS RIESGOS, COMO EN MEDIR LA EFICACIA DE LOS PROPIOS CONTROLES.

5. NORMATIVAS MÁS FRECUENTEMENTE UTILIZADAS PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA

SE DENOMINA **SEGURIDAD FÍSICA** AL ESTADO QUE ALCANZAN LAS INSTALACIONES DONDE SE VISUALIZA, AMACENA, PROCESA O TRANSMITE INFORMACIÓN CUANDO SE LE APLICAN UN CONJUNTO DE MEDIDAS EFICACES DE PROTECCIÓN PARA PREVENIR O BIEN EL ACCESO A LA INFORMACIÓN DE PERSONAS NO AUTORIZADAS O LA PÉRDIDA DE ESTA.

DEBERÁN DARSE LAS CONDICIONES ADECUADAS PARA QUE SE MANTENGAN LAS CONDICIONES DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN.

LA IMPORTANCIA QUE TIENE LA SEGURIDAD Y EL CRECIENTE USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN HA LLEVADO A CREAR UN MARCO LEGAL Y JURÍDICO CUYO OBJETIVO ES PROTEGER EL USO Y EL INTERCAMBIO DE INFORMACIÓN.

5. NORMATIVAS MÁS FRECUENTEMENTE UTILIZADAS PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA

EN CONCRETO, EN MATERIA DE SEGURIDAD FÍSICA, SERÁN APLICABLES COMO MEDIDAS DE CONTINGENCIA ANTE LOS POSIBLES RIESGOS LA NORMATIVA APLICABLE A LAS EDIFICACIONES TÉCNICAS:

- LEY 38/1999, DE 5 DE NOVIEMBRE, DE **ORDENACIÓN DE LA EDIFICACIÓN**.
- REAL DECRETO 513/2017, DE 22 DE MAYO, POR EL QUE SE APRUEBA EL **REGLAMENTO DE INSTALACIONES DE PROTECCIÓN CONTRA INCENDIO**S.
- REAL DECRETO 314/2006, DE 1 7 DE MARZO, POR EL QUE SE APRUEBA **EL CÓDIGO TÉCNICO DE EDIFICACIÓN**, QUE ESTABLECE LAS EXIGENCIAS QUE DEBEN CUMPLIR LOS EDIFICIOS EN CUESTIONES DE SEGURIDAD Y HABITABILIDAD.
- LA **NORMA ISO 27002:2022**, QUE ESTABLECE LOS CONTROLES DE SEGURIDAD FÍSICA Y DEL ENTORNO.
- **ANSI/TIA-942-B** (TELECOMMUNICATIONS INFRASTRUCTURE STANDARD FOR DATA CENTERS ESTA **NORMATIVA ES ESPECÍFICA PARA LOS CPD, CENTROS DE PROCESOS DE DATOS)** Y EN ELLA SE ESPECIFICAN LOS REQUISITOS MÍNIMOS QUE DEBE TENER UNA UBICACIÓN FÍSICA PARA CONTENER EN ELLOS EQUIPOS PARA EL ALMACENAMIENTO DE INFORMACIÓN.

CONTENIDOS

1. INTRODUCCIÓN
2. NORMA ISO 27002. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
3. METODOLOGÍA ITIL. LIBRERÍA DE INFRAESTRUCTURAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN
4. LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
5. NORMATIVAS MÁS FRECUENTEMENTE UTILIZADAS PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA

RESUMEN

LA INFORMACIÓN ES UN ACTIVO MUY VALIOSO EN CUALQUIER ORGANIZACIÓN Y MÁS EN UN MUNDO GLOBALIZADO EN EL QUE ESTA PUEDE CIRCULAR POR LOS CINCO CONTINENTES EN CUESTIÓN DE SEGUNDOS.

LA NORMA **ISO/IEC 27002** ES UNA GUÍA DE BUENAS PRÁCTICAS EN LA QUE SE INCLUYE UNA SERIE DE MEDIDAS Y CONTROLES DE SEGURIDAD QUE LAS ORGANIZACIONES

DEBEN TENER EN CUENTA PARA QUE SE ELABOREN, IMPLANTEN Y DIFUNDAN (EVALUACIÓN DE RIESGOS, SEGURIDAD EN LOS RECURSOS HUMANOS, GESTIÓN DE LOS ACTIVOS, ETC.). ES NECESARIO ESTABLECER UN NIVEL ADECUADO DE SEGURIDAD FÍSICA TANTO EN LAS ÁREAS SEGURAS DE UNA ORGANIZACIÓN COMO EN LOS EQUIPOS QUE FORMAN PARTE DE ELLA.

RESUMEN

ADEMÁS DE TENER EN CUENTA LAS RECOMENDACIONES DE LA NORMATIVA **ISO/IEC 27002**, UNA ORGANIZACIÓN DEBE SABER CÓMO PODER INTEGRAR LAS TECNOLOGÍAS DE LA INFORMACIÓN EN TODOS SUS PROCESOS.

PARA ELLO ESTÁ LA BIBLIOTECA DE INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN (**ITIL**), UN **CONJUNTO DE BUENAS PRÁCTICAS** QUE TIENE COMO OBJETIVO AYUDAR A ALCANZAR UNA BUENA GESTIÓN DE LOS SERVICIOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN.

APARTE DE UNA CORRECTA INTEGRACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN LOS PROCESOS DE UNA ORGANIZACIÓN, HAY QUE SER ESPECIALMENTE METICULOSO CON LOS DATOS DE CARÁCTER PERSONAL QUE SE PUEDAN TRATAR, YA QUE LA PROTECCIÓN DE LOS DATOS PERSONALES ES UN DERECHO FUNDAMENTAL QUE TIENEN LAS PERSONAS, REFLEJADO EN LA CONSTITUCIÓN ESPAÑOLA.

ESTO ES TODO